University of Piraeus

Department of Digital Systems

MSc in “Digital Systems Security”

«Security Policies for e-voting systems»

Maria Karagiassoti [MTE1208]

Supervisor: Konstantinos Lambrinoudakis, Associate Professor

University of Piraeus

Academic Year 2012-2013

Outline

Figures

Acknowledgements

This thesis was completed as a result of my studies at Digital Systems Security Master Program of University of Piraeus. I would like to thank my supervisor professor Konstantinos Lamprinoudakis for his guidance and support. Finally, I would like to thank my family and fellow students for their understanding and support.

Abstract

The ever-growing service delivery in electronic government (e-government) in conjunction with the wide immersion of Information and Communication Technologies (ICT) in public sector has underlined the need for reconsideration of the security measures that ensure the inner transactions. Electronic voting represents one of the most common examples of e-government application. The challenge that imposes the ability of citizens to exercise their voting rights in terms of security is imperative. Thus, security experts need to ensure the e-voting processes so as to provide a secure service to citizens. The main principles that must be reflected to the security policies of the system are also identified in the conventional voting systems. The current thesis has used those principles, as well as others imposed by the nature of the system, to model and develop an e-voting system. The functional requirements were the basis of the designed system and of its security policy. The development of the e-voting system was performed by utilizing theWSO2 Identity Server platform, while the security policies were implemented in the XACML language.

E-Voting

E-voting service worldwide

Progress in online service delivery continues in most countries worldwide. Electronic government (e-government) innovation that encompasses information and communications technologies (ICT) has lately increased. Specifically, technology solutions have gained special recognition as the means to serve economic and social sectors. However, according to United Nations E-Government Survey[1] the general recessionary world climate has resulted in a reduction to e-government investments.

The direct democratic participation is encouraged through online voting and interactive polling. Decision-making procedures can be enhanced by the application of an electronic voting service to evaluate citizens' decisions in matters of local or national government.

The digestion of e-voting solutions worldwide is undeniable. In 2011 people of United Arab Emirates experienced e-voting using kiosk machines in the federal national council elections, in Saudi Arabia. Furthermore, they are studying adopting e-voting in the next municipality's elections. Estonia is an also a country that has adopted Internet voting in presidential and Parliament elections since 2005. Other countries like Norway and Australia have adapted Internet voting partially. In the last year also Egyptians abroad experienced remote voting through postal service which was also tried in Estonia before adopting Internet voting.

Advances have also been made in open source are regarding e-voting software. Helios is a representative open-source web-based e-voting application. On the other hand, Norway published the source code of its e-voting system.

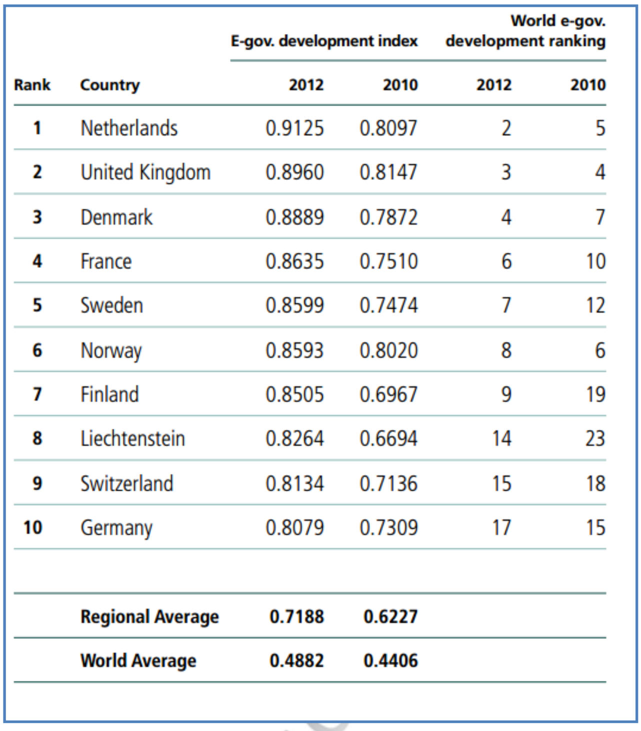
The Single Transferable Vote (STV) system in e-voting, allows voters to indicate the candidates of their preference, and rank them in order of preference.

E-voting service in Europe

The European region has the highest level of e-government development, which is around 50 percent higher than that of the world as a whole. Western and Northern Europe offer the most online services but considerable gains were also made by Southern and Eastern Europe as

[1] *E-Government Survey 2012, E-Government for the people – United Nations http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf*

well as in 2012. Especially in the context of *Europe 2020* the innovative use of technology in order to serve economic growth, employment, education, social inclusion and climate, is a key strategy.



		E-gov. development index		World e-gov. development ranking	
Rank	**Country**	**2012**	**2010**	**2012**	**2010**
1	Netherlands	0.9125	0.8097	2	5
2	United Kingdom	0.8960	0.8147	3	4
3	Denmark	0.8889	0.7872	4	7
4	France	0.8635	0.7510	6	10
5	Sweden	0.8599	0.7474	7	12
6	Norway	0.8593	0.8020	8	6
7	Finland	0.8505	0.6967	9	19
8	Liechtenstein	0.8264	0.6694	14	23
9	Switzerland	0.8134	0.7136	15	18
10	Germany	0.8079	0.7309	17	15
	Regional Average	**0.7188**	**0.6227**		
	World Average	**0.4882**	**0.4406**		

Table 1: Top 10 in Europe

(http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf**)**

Several case studies suggest that e-voting might serve as a powerful tool to augment the participation rate, the quality of voting, and aid in the implementation of political rights. In Europe, the introduction of information technology has been set as a major goal. Specifically, the *eEurope* initiative and action plan known also as ‘An information society for all’ initiative started under the European Governments. The application of digital technologies has become a vital factor for growth and employment in the new economy, mainly driven by the Internet. In spite of Europe’s leading role in certain technologies (mobile communications and digital TV, the uptake of the Internet in Europe remains comparatively low.

According to the E-Government Survey (2012), Europe has the largest share of the top e-participation countries. Despite the progress the gains are not spread evenly, both across and within countries, with the majority still offering low levels of engagement possibilities.

E-participation also requires the development of an e-culture among European citizens. Only technology aware and trained citizens will be able to take full advantage of the capabilities that e-government provides.

E-voting system

The first e-voting systems were designed so as to implement the main principles of 'paper-form' voting. The conventional process requires voters being successfully identified as eligible before proceeding to voting. In terms of e-voting processes, there are two types provided, based on the location of the voting process.

The first e-voting scheme requires that citizens must visit a polling station in order to vote. The identification stage has been preceded and voters can make use of their identification cards. The second type of E-voting system is based on remote technology. Usually voters have the chance to vote by using computers at remote locations or at polling stations. They use computer and internet networks in order to be able to access the system. Direct-recording electronic (DRE) voting machines are also serving the e-voting process, providing a robust system that increases the speed of vote counting. Voters can vote out of the normal interval for voting (usually office hours). They can also, vote from abroad. These constitute the most important advantage of the remote-based voting system. This idea is usually called I-Voting.

Structure

The e-voting system process incorporates several stages that serve different purposes. Most of the stages listed below derive from the classic voting procedure.

- Administration

The e-voting system's administrators are usually government's officers which are responsible for the preparation of the system, the supervision of the system's state as well as authorization and validation rights over the other users.

- Identification

The stage of identification involves the checks that are performed in order to ensure that a citizen is eligible to vote. The conventional voting process uses lists of eligible citizens, which must be identified when they arrive at the polling stations.

- Voting

The main voting process is encountered in this stage. Eligible citizens are able to cast their vote while the secrecy of their ballots is preserved.

- Tallying

The process of tallying involves the survey of all submitted ballots in order to determine the results of the elections taking into account only the valid ballots.

- Reporting

Reporting process involves the transmission of the results of the tallying process. The reporting process is also crucial as it must provide the integral output of the voting procedure.

Access Control

The complexity of sophisticated systems and collaborative infrastructures require the use of agile technology solutions that serve the communication of data among them. The most common format that serves this kind of information exchange is the eXtensible Markup Language or XML. XML provides an extensible structure for documents that is machine readable and easy to process, combined with the ability to design and develop schemas for document instance validation. The resulting creation of XML standards for representations and their use by collaborative systems dictate the need for a new layer of functionality: the ability to secure and enforce access control of the information from local data sources in a global manner.

Thus, the eXtensible Access Control Markup Language (XACML) enforces the security policies to a system, using XML schemas and instances. The security framework provides customization and filtering of XML instances, access control to the authorized users and as well as authorization classification. Towards the aforementioned approach, National Institute of Standards and Technology published the NIST RBAC model (Sandhu, Ferraiolo, and Kuhn, 2000) which was later adopted as an ANSI/INCITS standard in 2004.

In addition to Role Based Access Control, the Attribute Based Access Control also implements access filtering to a system's resources, through the evaluation of user attributes. Specifically, user profiles can be customized depending on the business requirements of the system. In terms of voting systems, the information regarding electoral districts, the age as well as the identification number of the user can be used as validation elements within security policies.

The combined use of role based and attribute based access control methodologies, provide a quick and efficient tool. Authorization conclusions are made either through the evaluation of attribute values that are known a priori to the system or after simple queries and comparisons of elements within the system.

An indicative example of the evolution of RBAC is the UCON (Usage Control) proposed by Park[2]. It integrates Authorizations, Obligations and Conditions and it was recognized as the latest major enhancement of the classic access control models, and drew considerable interest and attention. The original UCON is made of six core components: subjects (with attributes), objects (with attributes), rights, authorizations, obligations, and conditions. The first three components are inherited from traditional access control models, and have similar meanings. The last three are new components for usage control decisions. Authorization permits or rejects a subject request based on the evaluation of the subject and/or the object attributes under conditions. Obligations are requirements a subject has to perform before or during his/her access. Conditions are system and environment constraints for decision, and independent of both subjects and objects attributes.

XACML Language

The "economics of scale" which have led to the reduction of cost, have also led computing platform vendors to develop products with a generalized functionality, so that they can be used in the widest possible range of situations. Thus, there is a need for a common language for expressing security policy. Modern platforms are designed so as to be agile as well as easily adopted in as many application environments as possible, including those with the most permissive security policies. According to XACML 3.0 specifications document "*XML is a natural choice as the basis for the common security-policy language, due to the ease with which its syntax and semantics can be extended to accommodate the unique requirements of this application, and the widespread support that it enjoys from all the main platform and tool vendors*".

XACML language is the OASIS (Advancing Open Standards for the Information Society) [3]standard for fine-grained authorization management. The methodologies that XACML implements are based on the concept of Attribute-based access control (ABAC), as well as Role Based Access Control (RBAC) when it comes to access control decisions.

The areas that XACML language covers can be summarized to the following areas:

[22] http://profsandhu.com/it962/it962s06/l2_ucon_paper_marked_up.pdf

[3] https://www.oasis-open.org/

- Policy Language

XACML is using authorization mechanisms for web services. It provides '*fine grained authorization*' which underlines the level of detail in the access control. Specifically, the policies do not rely only on resources and XACML also defines set of functions, which can be used in authorization logic evaluation.

- Request-Response Protocol

The request/response language expresses queries about whether a particular request for access to a resource should be permitted (request) and describes answers to those queries (response). Policies are defined in terms of subjects and resources while attributes also have an integral role. Both subjects and resources are identified using URIs.

- Reference Architecture

The XACML architecture provides a standard for the deployment of necessary software modules to achieve efficient enforcement of XACML policies. The core components are depicted in Figure 1 while a detailed description of the components and the workflow can be found in Architecture section.

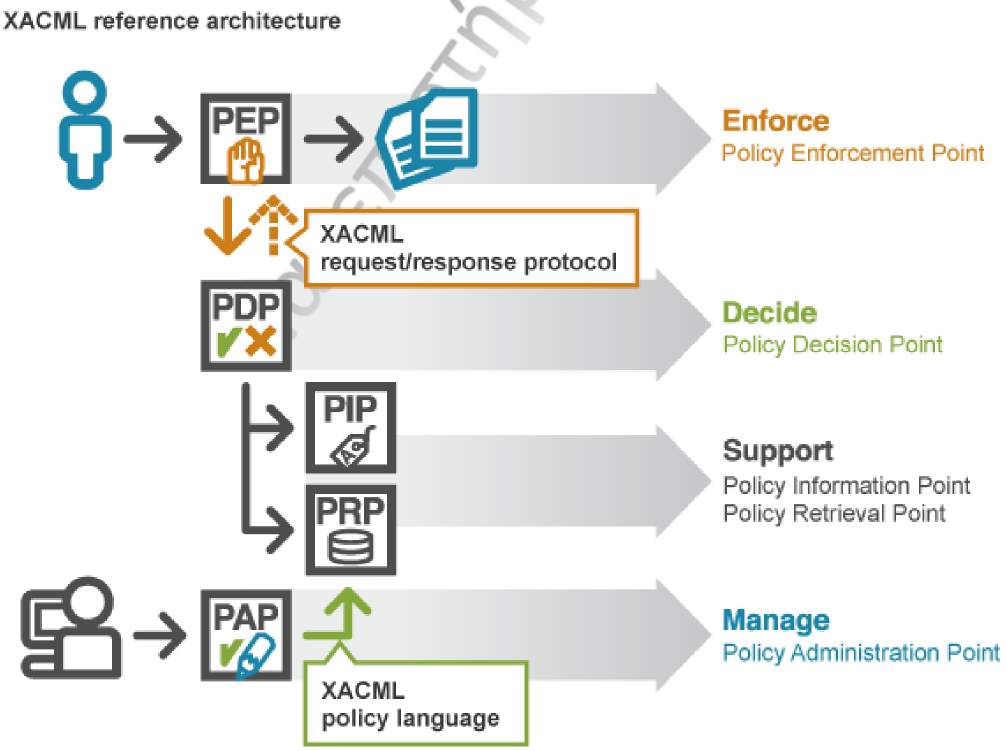


Figure 1: XACML Reference Architecture (Source:https://www.axiomatics.com/)

XACML implements a series of functionalities which are compliant to ISO/IEC 10181-3 which refers to the Access control framework of Open Systems Interconnection.

Architecture

The complete policy applicable to a particular decision request may be composed of a number of individual rules or policies. Each user can define different aspects to a policy. Thus, it is essential that the separate policies to be combined to a single policy applicable to the request. The top-level policy elements that constitute the policy enforcement model in XACML are <Rule>, <Policy> and <PolicySet>.

The *Rule* is the basic element of management which evaluates a Boolean expression and returns the result. Those expressions refer to the operators of the system, the resources, the subjects, the environment, the actions as well as the attributes. Subjects are the actors that are to perform an action. The system usually links several attributes to its users which can be used during the evaluation process. However, rules cannot be accessed by the Policy Decision Point (PDP) of the architecture, so it cannot provide authorization decisions itself.

Unlikely, *Policy* element can include one or more rules that returns the result of the evaluation of the rules. The combining algorithms provided by XACML are the following:

- Extended Indeterminate values
- Deny-Overrides
- Ordered-deny-overrides
- Permit-Overrides
- Ordered-permit-overrides
- Deny-unless-permit
- Permit-unless-deny
- First-applicable
- Legacy Deny-overrides
- Only-one-applicable

The Policy element is the basic unit of policy used by the PDP in terms of policy enforcement within the system.

PolicySet element is constituted by one or more Policy or PolicySet elements. The role of the PolicySet is to combine the results provided by its components.

The basic components that participate in the policy enforcement procedure are listed below:

Policy Administration Point (PAP)

The system entity that creates a policies or/and policy sets and then provides them to the Policy Decision Point (PDP) in order to evaluate them.

Policy Decision Point (PDP)

PDP is the system component that uses the policies from PAP and information provided from the PIP to evaluate policies and render an authorization decision.

Policy Enforcement Point (PEP)

The system entity that performs the access control, by making decision requests to the PDP and enforcing authorization decisions.

Policy Information Point (PIP)

The system entity that acts as a source of attribute values. That information is provided to the PDP in order to proceed to the evaluation of a policy.

The data flow that takes place within the system is depicted in the following figure:

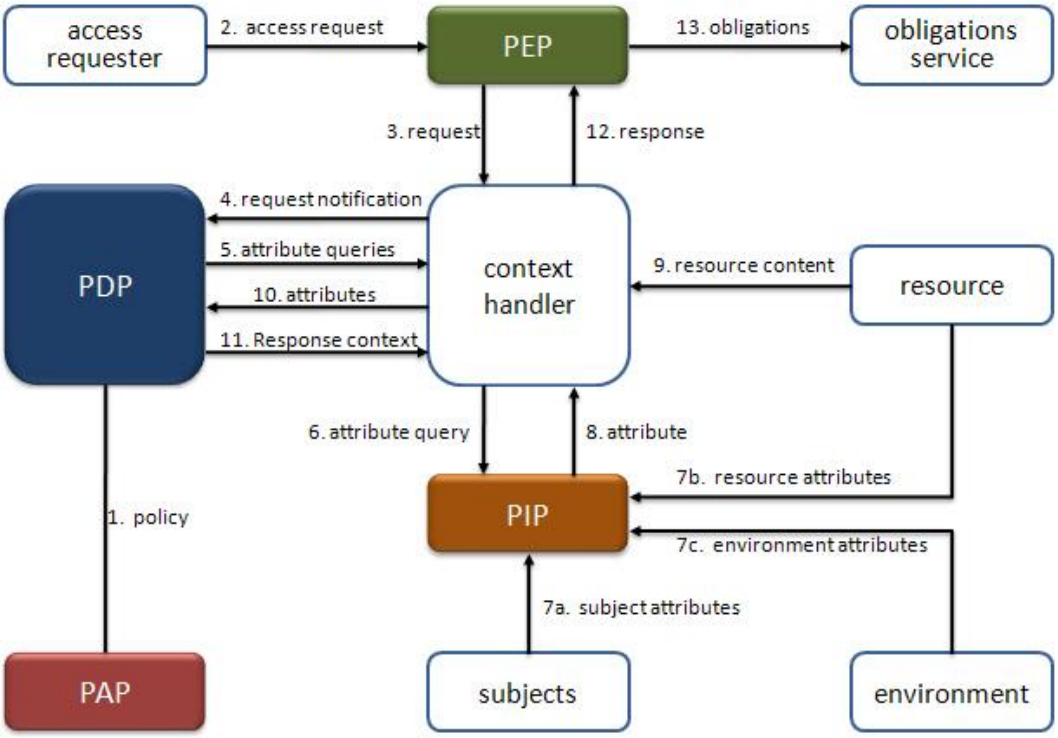


Figure 2: Data Flow (Source: http://docs.oasis-open.org/)

Initially, the requester demands access to a particular resource from the Policy Enforcement Point (PEP). The PEP forwards the request to the context handler which is the responsible node for management of requests, including information such as attributes of the subjects, resource, action and environment. Then, the request is provided to the Policy Decision Point which evaluates the request based on the policies that have been defined at the Policy Administration Point (PAP). Subsequently, the PDP requests from the context handler further information regarding subject, resource, action, environment and other categories attributes. The Policy Information Point (PIP) retrieves the requested information and returns them to the context handler which in its turn returns them to the PDP. Since the PDP has all the needed information available, it can evaluate the policy and return the result to the PEP through the context handler. Consequently, if the response is positive, the PEP allows the requester the access to the resource. Otherwise, the access is denied.

WSO2 Identity Server

The e-voting system that was developed in the framework of this thesis utilized theWSO2 Identity Server (WSO2 IS)[4] as its implementation platform. The Identity Server is based on

[4] http://wso2.com/products/identity-server/

WSO2 Carbon, the core platform of middleware products. Its main purpose is to offer Identity Management and Entitlement services. Also, it provides functionalities which include the use of Open ID, SAML2, WS-Trust, XACML 2.0, role based (RBAC), attribute based (ABAC) as well as policy based access control.

WSO2 Identity Server facilitates the identity management among employees, vendors, partners and customers across internal, shared, and Software as a Service platforms. It provides a single sign-on environment that can be customized to the user needs. Moreover, the use of methodologies as role-based access control (RBAC) convention and fine-grained policy-based access control facilitate the identity and entitlement management as well as the administration.

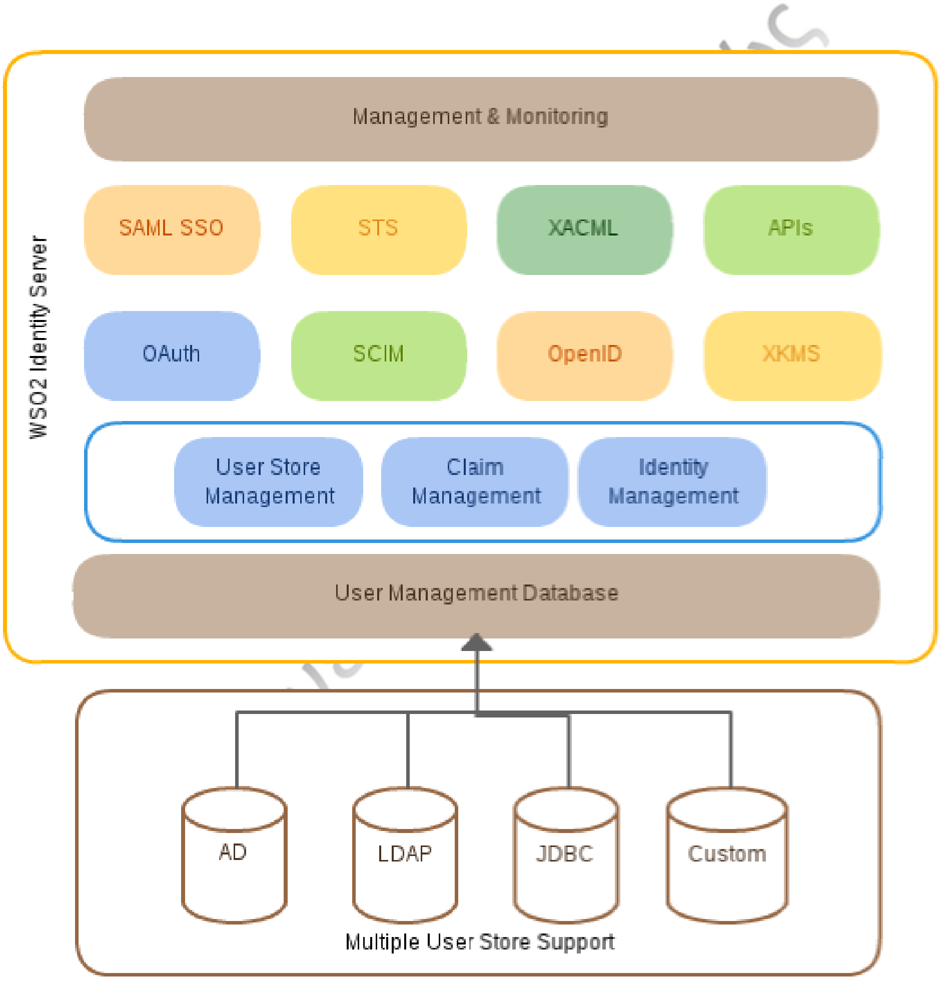


Figure 3: WSO2 IS Components (Source:https://docs.wso2.org/)

System Requirements

In the context of the current thesis, an e-voting system was developed and used as a case study. The specifications of the developed system were defined after studying implemented e-voting systems, as well as analyzing the processes taking place during the conventional – "paper-based" – elections. Unlike the conventional voting systems, an e-voting system involves extra parameters that need to be considered. However, the main principles that underline the democratic nature of the voting process are applicable in both cases.

The functional requirements that refer to the electronic voting system can be identified as functional and non-functional requirements. Initially, the e-voting system must be in accordance to the legal framework of the country. Requirements as the abolition of under aged or citizens that have been attainder of their civil rights from the voting process must also be reflected in the electronic voting system. Moreover, the system must ensure its users in terms of confidentiality of their vote, integrity of the ballot files both before and after the voting process, as well as availability of the resources during the voting process.

The requirement of *privacy* is vital part of an election process regardless the type of the system. Voters are free to vote the parties and representatives of their choice, while being assured that those choices will not be disclosed.

In the context of privacy, the voting process needs to guarantee the secrecy of their votes. However, it is crucial that ballot files are appropriately maintained so as not to reveal the user that submitted them. *Unlinkability* between voter and ballot is a requirement that is implemented through the use of several techniques and security protocols.

Voters need to have the ability of anonymous voting while at the same time will be ensured that their ballot file was valid and successfully submitted. Voting receipts can be a solution in the first place; however coercibility and bribe can put the democratic process in danger. Thus, e-voting systems need both receipt-freeness and efficiency. A methodology that is proposed in these cases, involves blind signatures. The scheme contains two kinds of participants, a signer and a group of users who request the signatures from the signer. The process involves a request from a user to the signer and the computation and issue of the blind signature by the signer.

Availability is also crucial for a voting process. As any e-government service, the appropriate measures need to be taken so as to ensure the robustness of the system. Especially while the voting process is active, any attack towards the e-voting system needs to be confronted successfully.

The content provided to end-users needs to be accurate and authentic. Ballot files as well as any system information provided to citizens must be ensured against any unauthorized access and modification. Thus, *integrity* needs to be maintained within the system.

In addition, the system must efficiently log any transaction performed within the system, so as either to prevent or confront successfully any security incidents. Thus, this functionality can also serve as a *non-repudiation* mechanism for both internal and external attacks.

Design Requirements

Functional requirements are the main point of reference which the developers will use in order to design and then implement the system. The requirements of privacy, authenticity and confidentiality require a system which will allow access only to authorized users. In particular, it is assumed that only authorized users have access to the system and identity verification processes have been preceded. Government officers have performed all appropriate checks according to the legislative framework and have proceeded in providing the credentials to the eligible citizens. Apart from the credentials, users are assigned to a particular role depending on their responsibilities within the system.

In order to achieve a better level of security, each user must be assigned to a specific user group or *Role*. Also, several attributes related to the locality or the responsibilities of the user, can be used in the access control policies. Information such as the electoral district he or she belongs can differentiate the access control among users belonging to the same group.

The criticality of the voting process requires constant monitoring of every change of the system state. Audit logging is essential, however it is mandatory that users with elevated privileges (i.e. election organizers, system administrators), must authorize users to access restricted resources. Only in cases the users fulfill the requirements, must they be permitted to access the resource.

Changes in the system state must also be subjected to validation. System administrators, for instance, must either permit or deny the closure of a poll from an election organizer, before the action is actually committed.

During the voting process, users must be able to access only their personal ballot files. The ballot file will be sent to a ballot pool when the user cast it and he or she will not be able to re-send it. Ballot files are assigned with a particular ballot ID which will only be used for integrity checks.

The *evote* system

Based on the requirements analyzed in the aforementioned sections, the *evote* system was developed in order to implement the defined functionalities through security policies within the system. The voting system was developed using WSO2 Identity Server, as a file system where each resource refers to a component of the voting system. It is implemented as a multi-purpose voting system, which can be used for general or internal elections, polls and plebiscites.

File Registry

The file system is developed under the ***_evote*** resource, which constitutes the super-directory of the e-voting system.

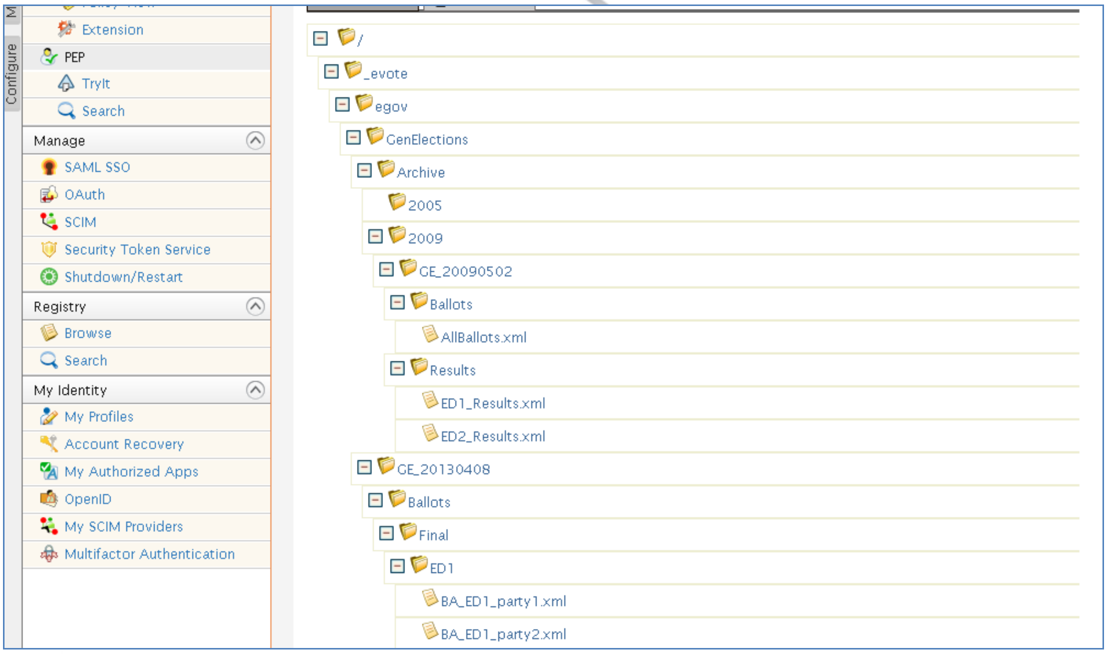


Figure 4: Evote File System [1]

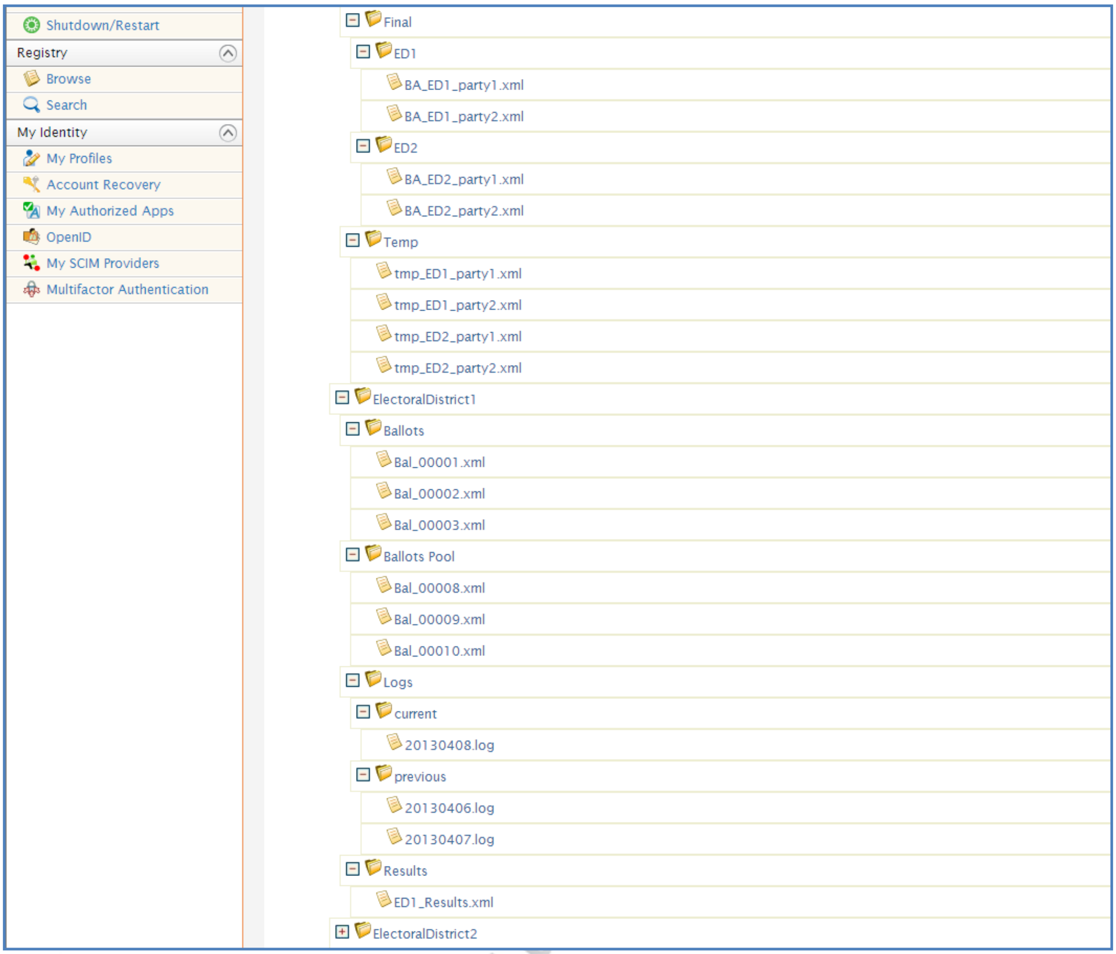


Figure 5: Evote File System [2]

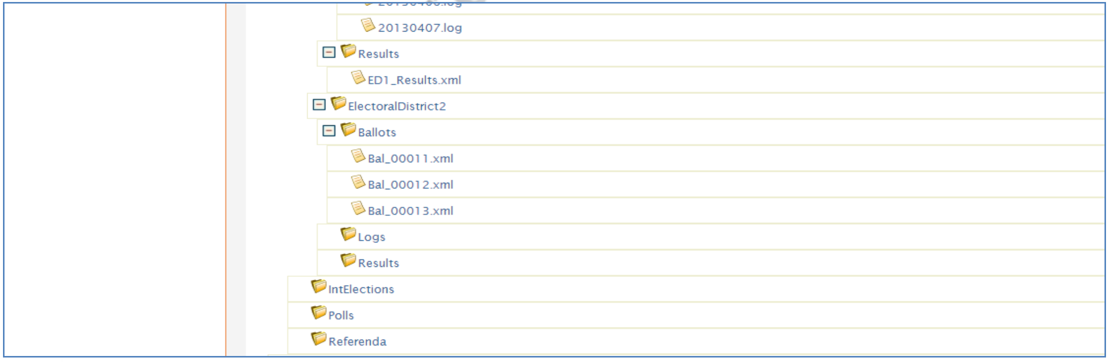


Figure 6: Evote File System [3]

The second layer includes the **egov** directory which indicates the resource which includes the e-government services' file system.

Thereafter, the actual file system is deployed. Specifically, the resources are divided into the following subcategories:

- Internal Elections

- Polls
- Referendum (plebiscite)
- General Elections

Internal Elections

Internal Elections resource refers to elective processes that involve decisions within the parties. Elections for leadership positions within a party will be maintained within the current resource.

Polls

The Polls resource incorporates all elective processes posed by the government to citizens regarding national matters.

Referendum (plebiscite)

In cases where the electorate is asked to either accept or reject a proposal. Citizens usually have to choose between two options; however the multiple choice referendums have also been used in several cases.

General Elections

The *GenElections* resource constitutes the subsystem that refers to general elections. The resource is constituted by the listed sub-resources:

- Archive resource, which includes the details of past general elections
- GE_20130408 resource, which includes the details of the currently open general election of the 8th of April.

Archive resource

All information regarding past general elections is maintained in the Archive resource, divided by the year of conducting. For instance the information regarding the general elections of 2009 is included in the corresponding folder *2009* under the name *GE_20090502*. Further details stored for informational purposes include:

- *Ballots*, which contains a consolidated file of all ballots per electoral district (*All_Ballots.xml*).
- *Results*, which contains all results per electoral district in separated files (*ED1_Results.xml*, *ED2_Results.xml*etc).

GE_20130408 resource

The subdirectory system under the name of *GE_20130408* refers to the currently open general election. Its name stands for the *General Election* initials as well as the date the elections take place. Further classification provides a better view of the information stored. Specifically:

- Ballots, which indicates the files related to ballots.
- Electoral Districts, which indicates the super-directory of all electoral districts.

Ballots

The resource of ballots maintains the details regarding the ballots per electoral district and party, as well as the ballots being processed (*Temp* subdirectory). Specifically, the representatives of each party will be able to alter temporary ballot files of their party and electoral district after being successfully identified as eligible by the system. However, there will be a limitation so as party representatives can edit the temporary ballots only until one week until the elections take place. Also, party representatives will be able to edit ballots of the party and electoral district they belong.

The final versions of ballots for all parties are listed per electoral district in the *Final* subdirectory. Those files cannot be edited by any user.

Electoral Districts

A crucial organizational part of the e-vote system relies on the electoral district resources. The structure provided for ElectoralDistrict1 in the following section is indicative and depicts the structure of all electoral districts within the system.

ElectoralDistrict1

The first electoral district can be accessed only by the voters and representatives belonging to the particular electoral district, as well as the users having an organizational or auditing role (Election Organizers, IT Auditors). The organizational structure can be summarized to the listed components:

- Ballots

  The ballot files of all citizens regarding the particular electoral district. The ballot files are represented as xml files which contain the information of the voter's choice. Ballot files are identified by their ID. Note that only one ballot file corresponds to each voter. A detailed description of the ballot file can be found in Appendix 1.

- Ballots Pool

  The ballot files that have been filled and submitted. The ballots cannot be edited and resubmitted by the user. The ballots in 'Ballots Pool' directory will be used in the tallying process when the voting process is finished.
- Logs
  - Current

    The log files of the current day.
  - Previous

    The log files of the previous days.
- Results

  The file containing the output of the tallying process and refers to the corresponding electoral district. Note that results of the voting process are available to all authorized users only when the tallying process is completed.

Attributes

Claims in WSO2 provide single and general notions to define the identity information related to a subject. Claim-based identity is a common way for any application to acquire the identity information. Thus, extra attributes were added in Claims repository (https://localhost:9443/carbon/claim-mgt/claim-view.jsp?store=Internal&dialect=http://wso2.org/claims) in order to support the access control. The following list enumerates the attributes added:

- Electoral District

  Electoral District attribute keeps the information of the electoral district that the user belongs. The electoral district is a read-only field.
- Ballot ID

  Ballot ID refers to the unique identification number of the ballot file of the user. The field is read-only.
- Vote Flag

  The vote flag indicates whether the user has voted or not. The value equal to '0' indicates that the user has not voted yet. Otherwise, the value '1' indicates that the user has voted, thus, he cannot vote again. The field is read-only.
- User ID

  The user identification number is a unique number assigned to each user. The field is read-only.
- Party

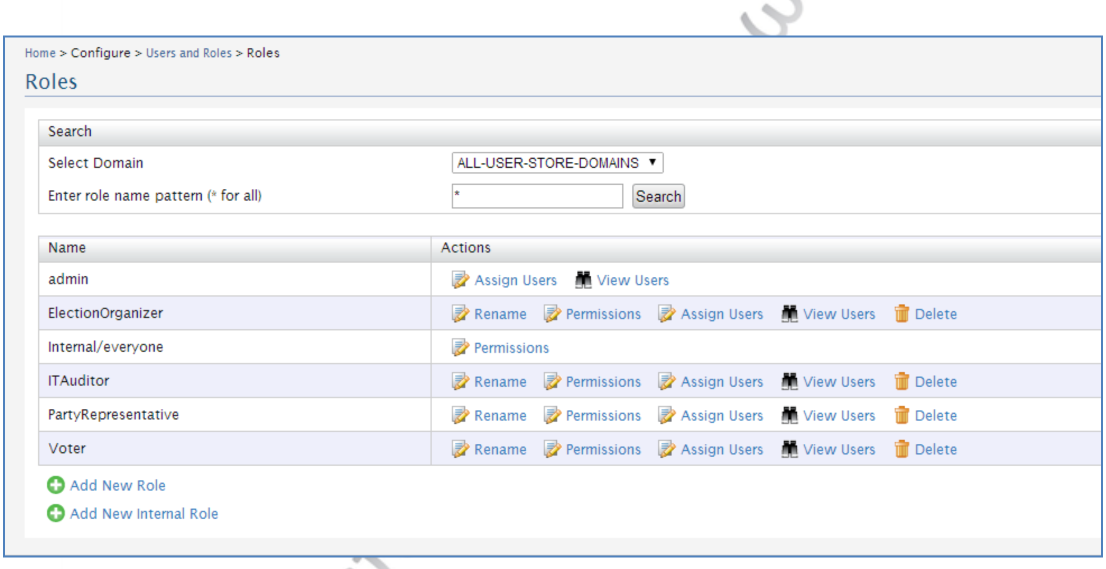
The party field indicates the party the user belongs. The information is applicable only to Party Representatives. Users having different roles are assigned the value ‘99’ to the particular field, which is read-only.

Roles

The users of the *evote* system are categorized into different groups currently referred as *Roles*.

Policies implement both Role Based Access Control (RBAC) as well as Attribute Based Access Control). As far as Role Based Access Control is concerned, roles have been created in order to provide the authorization on resources is performed through the classification of users in groups – the roles.

(*Admin* and *internal/everyone* are automatically generated by the platform)



Home > Configure > Users and Roles > Roles

Roles

Search

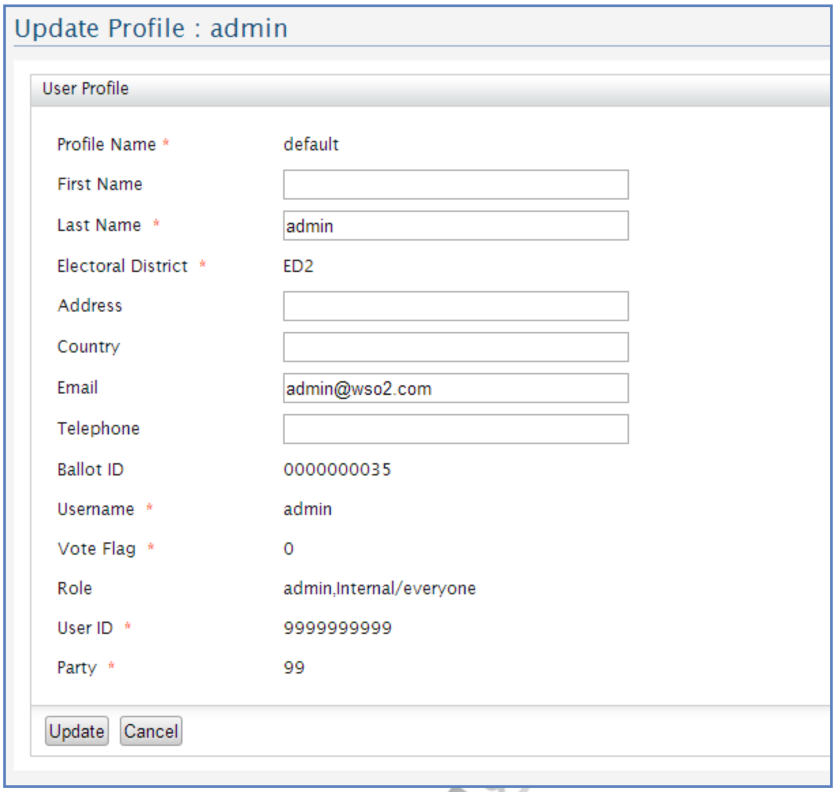
Select Domain	ALL-USER-STORE-DOMAINS ▾
Enter role name pattern (* for all)	* [Search]

Name	Actions
admin	Assign Users · View Users
ElectionOrganizer	Rename · Permissions · Assign Users · View Users · Delete
Internal/everyone	Permissions
ITAuditor	Rename · Permissions · Assign Users · View Users · Delete
PartyRepresentative	Rename · Permissions · Assign Users · View Users · Delete
Voter	Rename · Permissions · Assign Users · View Users · Delete

Figure 7: Roles of evote system

Admin

The system administrators are the system’s super-users whohave an overview of the *evote* state and act on it. Administrators are also eligible for auditing the actions of election organizers. Their role is more monitoring than functional within the e-voting system.



Update Profile : admin

User Profile

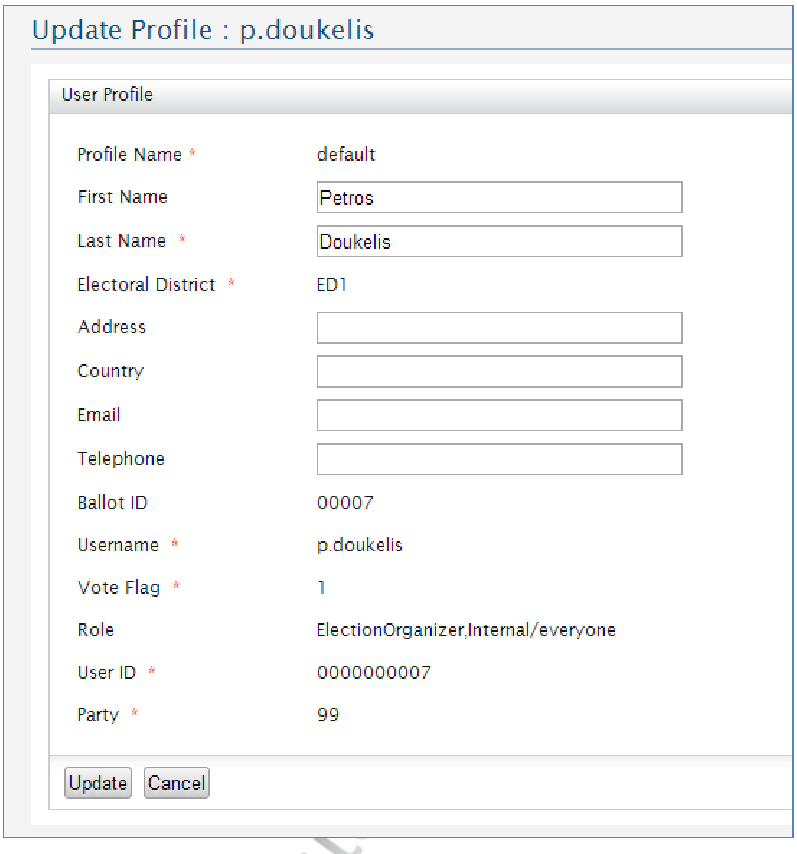
Profile Name *	default
First Name	
Last Name *	admin
Electoral District *	ED2
Address	
Country	
Email	admin@wso2.com
Telephone	
Ballot ID	0000000035
Username *	admin
Vote Flag *	0
Role	admin,Internal/everyone
User ID *	9999999999
Party *	99

Figure 8: Admin User Profile

Election Organizer

Election Organizer is responsible for the organizational tasks of an e-voting process. Specifically, election organizers areeligible for:

- Creating, modifying and deleting an e-vote process (General Elections, Internal Elections, Polls and Referenda). The action of deletion is only applicable to past processes (*Archive* section).
- Creating, modifying and deleting an electoral district. The actions of modification and deletion are only applicable to past e-voting.
- Viewing the results after the tallying process.
- Authorizing users to access specific resources.
- Validating changes in specific resources.



Update Profile : p.doukelis

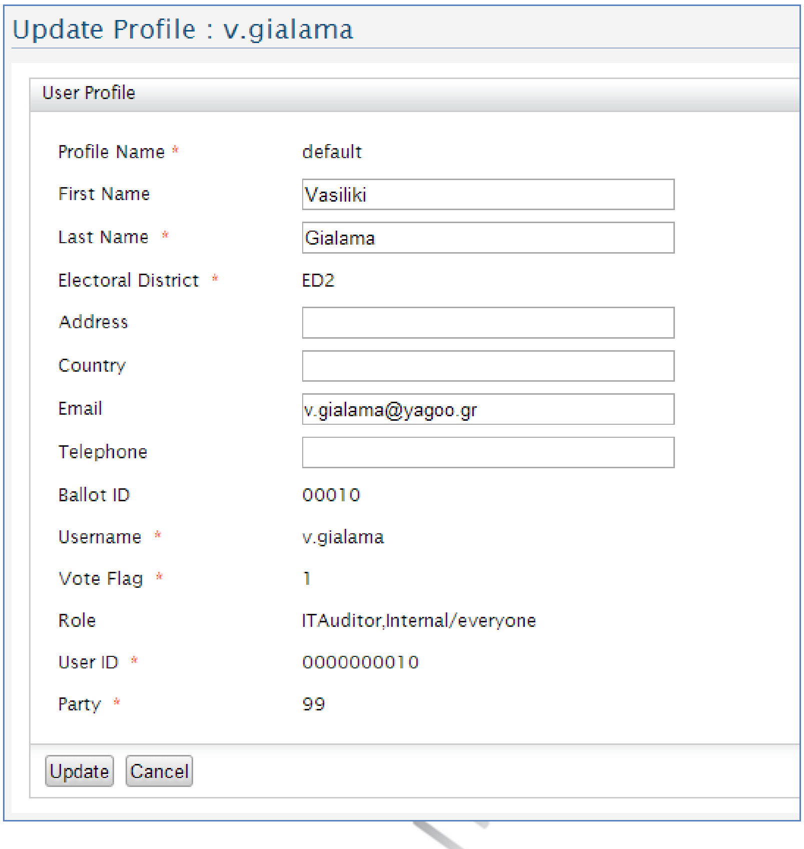
User Profile

Profile Name *	default
First Name	Petros
Last Name *	Doukelis
Electoral District *	ED1
Address	
Country	
Email	
Telephone	
Ballot ID	00007
Username *	p.doukelis
Vote Flag *	1
Role	ElectionOrganizer,Internal/everyone
User ID *	0000000007
Party *	99

Figure 9: Election Organizer User Profile

IT Auditor

The role of IT Auditor is both monitoring and functional within the e-vote system. The effective monitoring of the ongoing voting procedures is essential to both system and network facilities. Thus the access in log files per electoral district is required to both categories, whereas actions of modification and deletion are prohibited in any case. Audit professionals will also be able to view the results after the tallying process.



Update Profile : v.gialama

User Profile

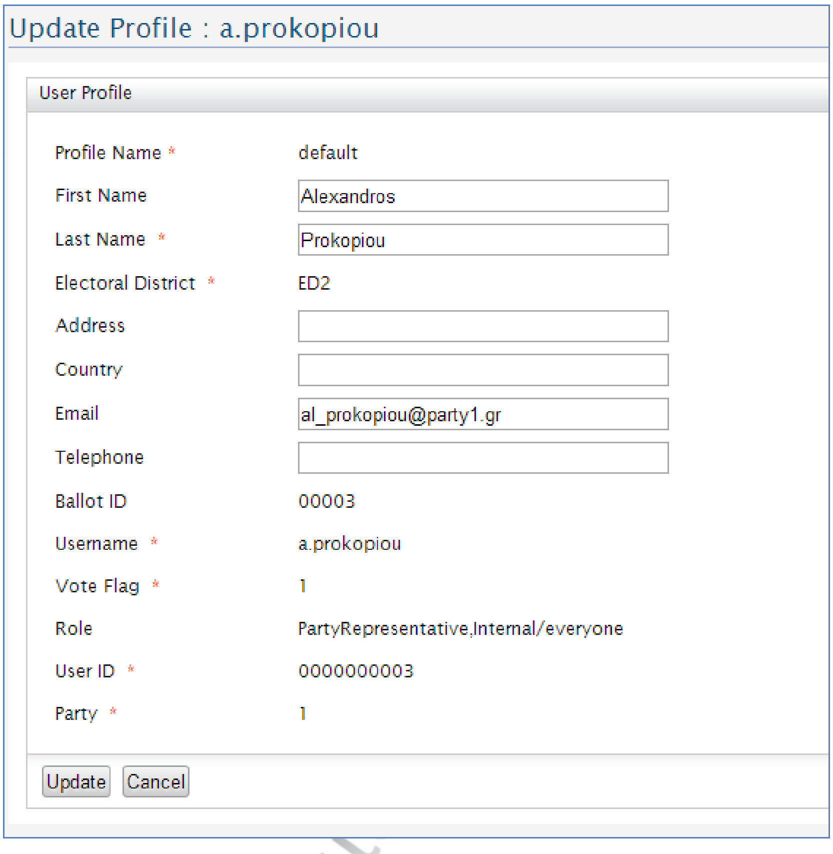
Profile Name *	default
First Name	Vasiliki
Last Name *	Gialama
Electoral District *	ED2
Address	
Country	
Email	v.gialama@yagoo.gr
Telephone	
Ballot ID	00010
Username *	v.gialama
Vote Flag *	1
Role	ITAuditor,Internal/everyone
User ID *	0000000010
Party *	99

Figure 10: IT Auditor User Profile

Party Representative

As in conventional voting process, parties must be represented in each electoral district, so as to assure the result of the tallying process. The party representatives are eligible for:

- The processing of the temporary ballot file of the party and electoral district they belong. This is achieved through the use of attributes in the user profile.
- Viewing the results after the tallying process.



Update Profile : a.prokopiou

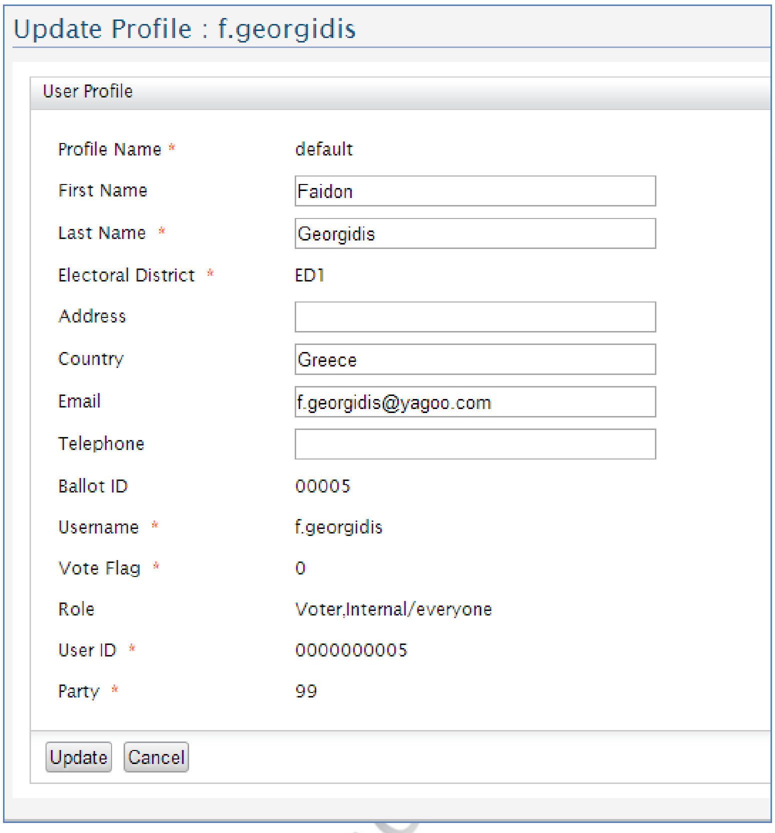
User Profile

Profile Name *	default
First Name	Alexandros
Last Name *	Prokopiou
Electoral District *	ED2
Address	
Country	
Email	al_prokopiou@party1.gr
Telephone	
Ballot ID	00003
Username *	a.prokopiou
Vote Flag *	1
Role	PartyRepresentative,Internal/everyone
User ID *	0000000003
Party *	1

Figure 11: Party Representative User Profile

Voter

The voters have only access to the ballots of the district they belong. Note that they are eligible for viewing only the final versions of ballots. Also, they are eligible for reading the tallying results, when the tallying process is finished.



Update Profile : f.georgidis

User Profile

Profile Name *	default
First Name	Faidon
Last Name *	Georgidis
Electoral District *	ED1
Address	
Country	Greece
Email	f.georgidis@yagoo.com
Telephone	
Ballot ID	00005
Username *	f.georgidis
Vote Flag *	0
Role	Voter,Internal/everyone
User ID *	0000000005
Party *	99

Figure 12: Voter User Profile

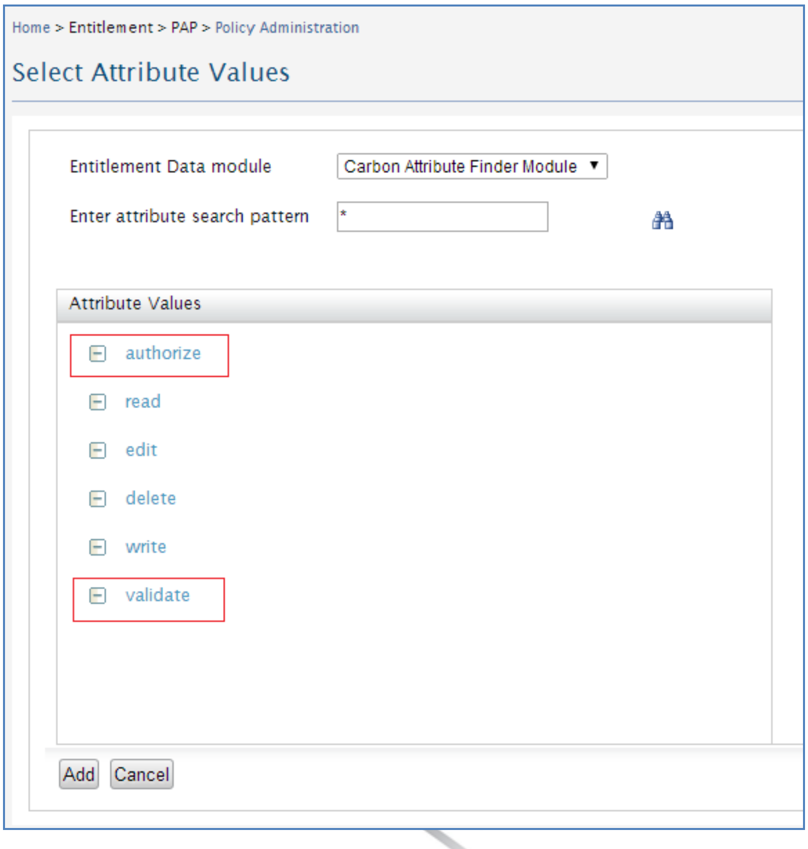
Actions

The *evote* system also supports a list of actions which the eligible users can perform to the system’s resources. The system-supported actions are:

- Read
- Write
- Edit
- Delete

In the context of the voting process and in order to enhance the levels of security within the system, two new actions were added to serve the purposes of authorization and validation[5].

[5] The modified code **CarbonEntitlementDataFinder.java** resides in \\wso2-source\source\components\identity\org.wso2.carbon.identity.entitlement\4.2.0\src\main\java\org\wso2\carbon\identity\entitlement\pap of WSO2 source code.



Home > Entitlement > PAP > Policy Administration

Select Attribute Values

Entitlement Data module: Carbon Attribute Finder Module ▼

Enter attribute search pattern: *

Attribute Values

- ⊟ authorize
- ⊟ read
- ⊟ edit
- ⊟ delete
- ⊟ write
- ⊟ validate

Figure 13: Action attribute values

Authorize

The authorization action is responsible for approving or not the action of a subject to a specific resource. Actually, resources that are not accessible to all users (ex. Log files) or actions that are not allowed to any user (modification of temporary ballot files), will be subjected to approval by the Election Organizers. Also, in case of Election Organizers' actions, the authorization will be given by the system's administrators (ex. Tallying process).

Validate

The action of validation will be performed in order to ensure that any system modification will be confirmed by another user with wider authority. For instance, changes in Election archives performed by Election Organizers must be also confirmed by the system's administrators. Also, changes in temporary ballot files will be confirmed by the Election Organizers.

The following table summarizes the permissions of each role regarding the action and the resource:

Action / Resource	Read	Edit	Write/Delete	Authorize	Validate
Archive	All	Election Organizers	Election Organizers	N/A	Admin
Temporary Ballots	Party Representatives	Party Representatives *	N/A	Election Organizers	Election Organizers
Final Ballot Files	All	N/A	N/A	N/A	N/A
Ballots (per Electoral District)	Voter*	Voter*	N/A	Election Organizer	Election Organizer
Ballots Pool (per Electoral District)	Admin, Election Organizer, IT Auditor, Party Representative	N/A	N/A	Election Organizer, Admin	N/A
Log Files	IT Auditor	N/A	N/A	Election Organizer	N/A
Results	All*	N/A	Election Organizer	N/A	Admin

The asterisk (*) indicates that the action is permitted to subject only when certain criteria are met.

Policies

The *evote* system's access control is implemented through the use of security policies which are authorizing users to perform actions on the system's resources. In this section are listed all the security policies implemented within the e-voting system. Moreover, for understanding purposes a case study of granted permission as well as denial is used per each policy (when applicable).

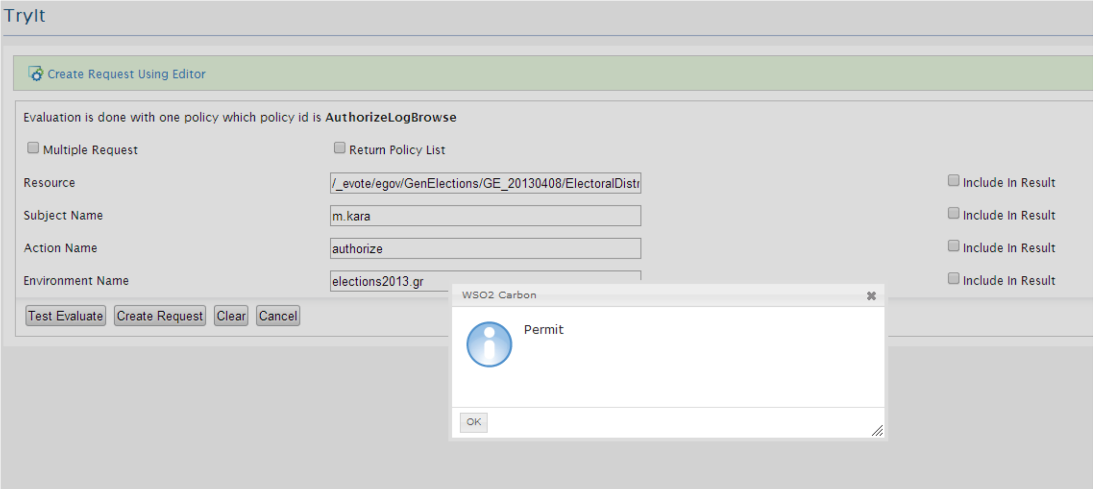
Policy	Actors	Resource	Description
AuthorizeLogBrowse	Election Organizers	Log Files	Election Organizers authorize IT Auditors to access the system's log files.
AuthorizeTallying	Election Organizers, System Administrators	Ballot files (Ballots Pool)	System administrators authorize election organizers and election organizers authorize IT Auditors and Party Representatives to access ballot files for tallying process.
AuthorizeTmpBallots	Election Organizers	Temporary Ballot files of a party	Election Organizers authorize Party Representatives to access temporary ballot files.
AuthorizeVoter	Election Organizers	Personal Ballot Files	Election Organizers authorize users to access their personal ballot file.
ManageArchives	Election Organizers	Archives	Election Organizers can add, edit or delete old elections' archives.
ManageEvote	Election Organizers	Evote system	Election Organizers can add, edit or delete resources within the evote system.
ManageTmpBallots_ ED11	Party Representatives of 1st party of ED1	Temporary ballot files of 1st party of ED1	Party Representatives belonging to the 1st party of ED1 can edit the temporary ballot files of their party and electoral district.
ManageTmpBallots_ ED12	Party Representatives	Temporary ballot files of 2nd party	Party Representatives belonging to the 2nd party of

	of 2nd party of ED1	of ED1	ED1 can edit the temporary ballot files of their party and electoral district.
ManageTmpBallots_ ED21	Party Representatives of 1st party of ED2	Temporary ballot files of 1st party of ED2	Party Representatives belonging to the 1st party of ED2 can edit the temporary ballot files of their party and electoral district.
Tallying_ED1	Party Representatives of ED1, IT Auditors, Election Organizers	Ballot files in Ballot Pool of ED1	Party Representatives of ED1, IT Auditors and Election Organizers are eligible for reading the ballot files of Ballots pool of ED1.
ValidateMngArch	System Administrators	Archives	System administrators validate any action that modifies the state of archives resources.
ValidateMngEvote	System Administrators	Evote system	System administrators validate any action that modifies the state of evote system’s resources.
ValidateModTBallots	Election Organizer	Temporary Ballot Files	Any change that is performed in temporary ballot files is validated by the election organizer.
ValidateTallying	System Administrators, Election Organizers	Tallying Results	System Administrators validate the outcome of the tallying process.
ValidateVote	Election Organizers	Personal ballot file	The voting process is validated by election

			organizers.
ViewArchives	All users	Archives	All users are allowed to read the archives.
ViewBallots	All users	Final ballot files	All users are allowed to view the final versions of ballot files.
ViewLogs	IT Auditors	Log files	IT Auditors are allowed to read the log files (current and previous).
ViewResults	All users	Results of voting process	All users are allowed to read the results of the voting process after the voting process is completed.
Vote	Voters	Personal ballot files	Each voter can edit its personal ballot file.

1. *AuthorizeLogBrowse*: Election Organizers are eligible for authorizing IT Auditors to access log files. Note that this action can only be performed from the domain '*elections2013.gr*'.

User	**m.kara (Election Organizer)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Logs/current/20130408.log
Action	Authorize
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **AuthorizeLogBrowse**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistr □ Include In Result

Subject Name: m.kara □ Include In Result

Action Name: authorize □ Include In Result

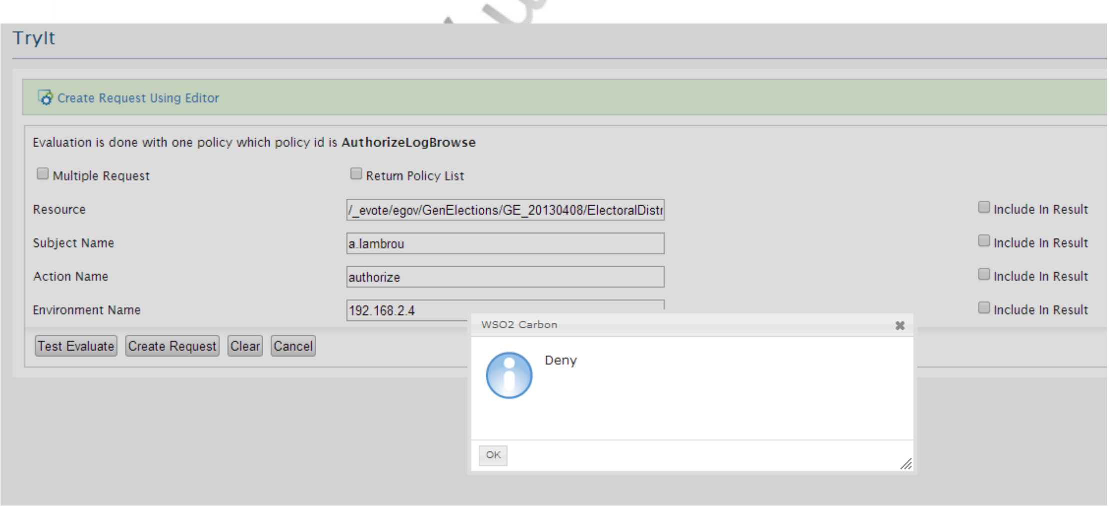
Environment Name: elections2013.gr □ Include In Result

WSO2 Carbon

Permit

Figure 14: Authorize Log Browse (Sucessful execution)

User	**a.lambrou (Party Representative)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Logs/current/20130408.log
Action	Authorize
Result	Deny



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **AuthorizeLogBrowse**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistr □ Include In Result

Subject Name: a.lambrou □ Include In Result

Action Name: authorize □ Include In Result

Environment Name: 192.168.2.4 □ Include In Result

WSO2 Carbon

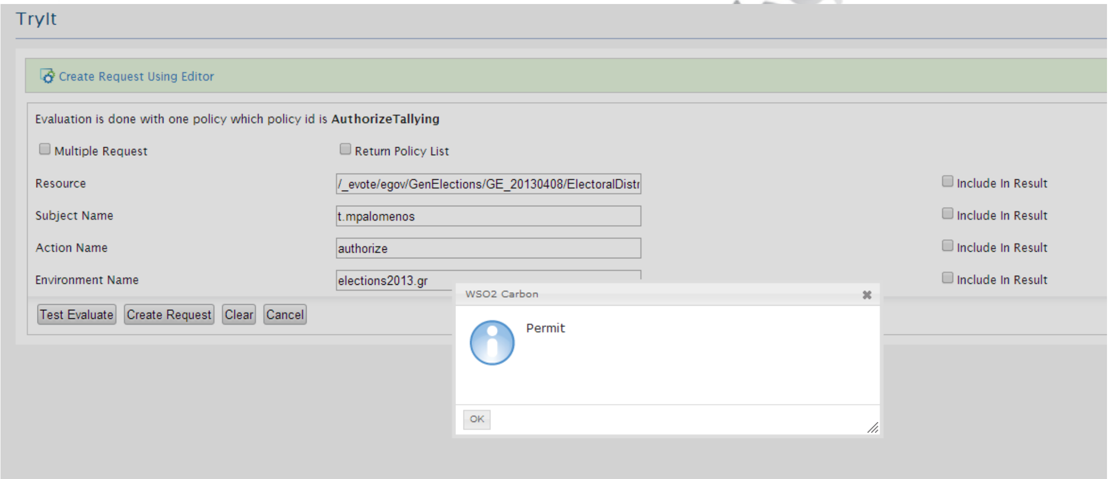
Deny

Figure 15: Authorize Log Browse (Unsucessful execution)

2. *AuthorizeTallying*: Election Organizers are eligible for authorizing IT Auditors and Party Representatives to access the Ballots Pool, in order to perform the tallying process. Also, system administrator is eligible for authorizing Election Organizers to access the Ballots Pool directory for tallying purposes. Both administrators and

Election Organizers are allowed to perform the authorization only from '*elections2013.gr*' domain.

User	**t.mpalomenos (Election Organizer)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots Pool/Bal_00008.xml
Action	Authorize
Result	Permit



Evaluation is done with one policy which policy id is **AuthorizeTallying**

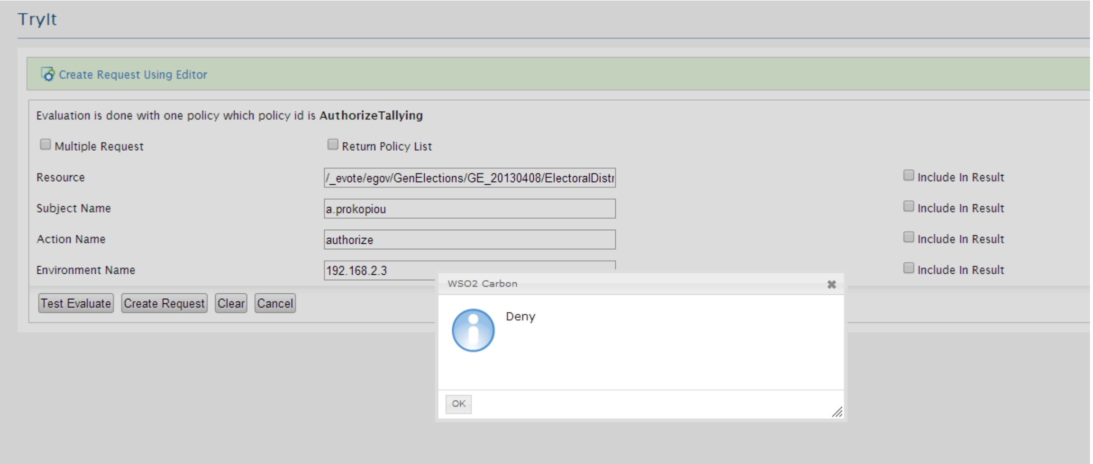
□ Multiple Request □ Return Policy List

Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistr	□ Include In Result
Subject Name	t.mpalomenos	□ Include In Result
Action Name	authorize	□ Include In Result
Environment Name	elections2013.gr	□ Include In Result

Permit

Figure 16: Authorize Tallying (Sucessful execution)

User	**a.prokopiou (Party Representative)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots Pool/Bal_00008.xml
Action	Authorize
Result	Deny



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **AuthorizeTallying**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistr □ Include In Result

Subject Name: a.prokopiou □ Include In Result

Action Name: authorize □ Include In Result

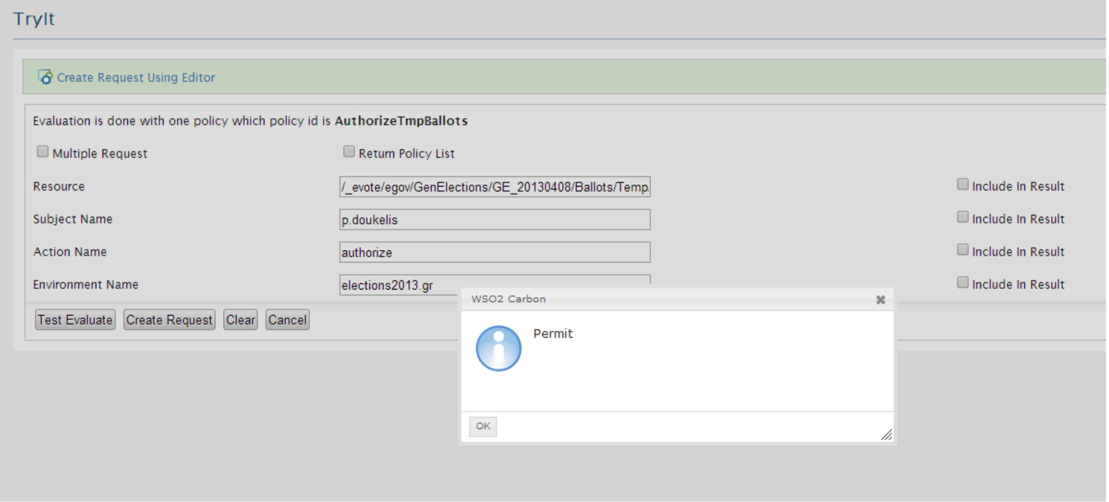
Environment Name: 192.168.2.3 □ Include In Result

Deny

Figure 17: Authorize Tallying (Unsucessful execution)

3. *AuthorizeTmpBallots:* Election Organizers authorize Party Representatives to access temporary ballot files in order to edit them. Note that this action is only allowed for domain '*elections2013.gr*'.

User	**p.doukelis (Election Organizer)**
Resource	/_evote/egov/GenElections/GE_20130408/Ballots/Temp/tmp_ED1_party1.xml
Action	Authorize
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **AuthorizeTmpBallots**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/Ballots/Temp □ Include In Result

Subject Name: p.doukelis □ Include In Result

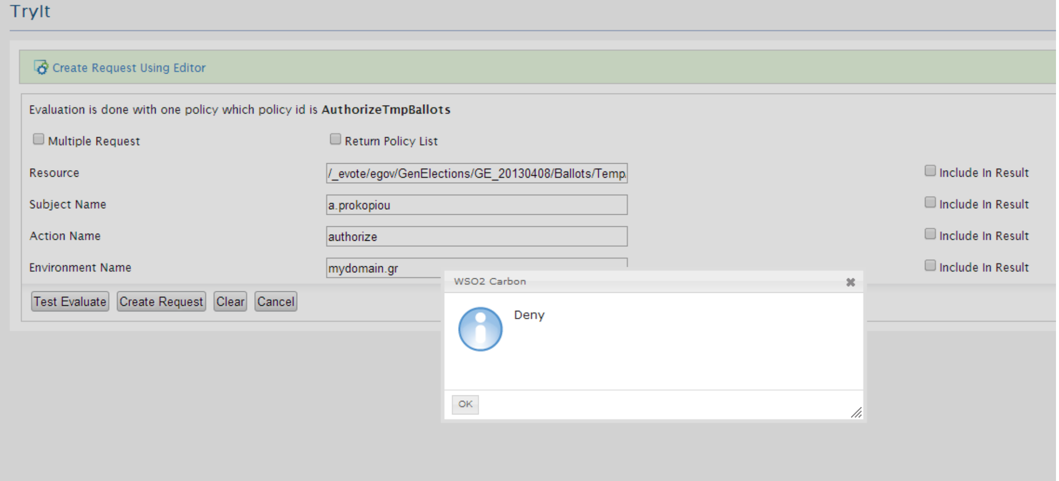
Action Name: authorize □ Include In Result

Environment Name: elections2013.gr □ Include In Result

Permit

Figure 18: Authorize Modifications in Temporary Ballots (Sucessful execution)

User	**a.prokopiou (Party Representative)**
Resource	/_evote/egov/GenElections/GE_20130408/Ballots/Temp/tmp_ED1_party1.xml
Action	Authorize
Result	Deny



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **AuthorizeTmpBallots**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/Ballots/Temp □ Include In Result

Subject Name: a.prokopiou □ Include In Result

Action Name: authorize □ Include In Result

Environment Name: mydomain.gr □ Include In Result

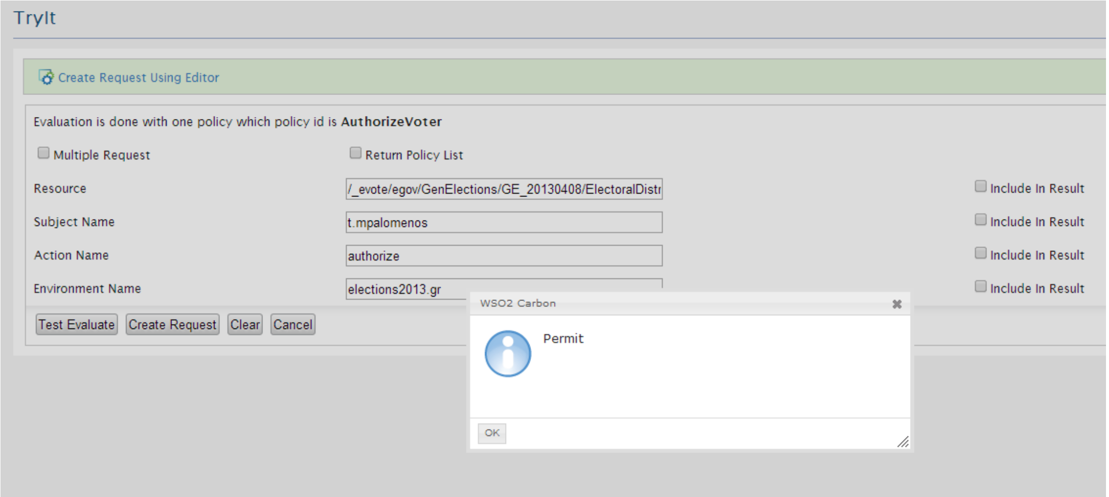
WSO2 Carbon

Deny

Figure 19: Authorize Modifications in Temporary Ballots (Unsucessful execution)

4. *AuthorizeVoter*: Election Organizers are eligible for authorizing Voters to access their ballot files. The domain from which the operation is applicable is the '*elections2013.gr*'.

User	**t.mpalomenos (Election Organizer)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots/Bal_00001 .xml
Action	Authorize
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **AuthorizeVoter**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistr □ Include In Result

Subject Name: t.mpalomenos □ Include In Result

Action Name: authorize □ Include In Result

Environment Name: elections2013.gr □ Include In Result

Test Evaluate | Create Request | Clear | Cancel

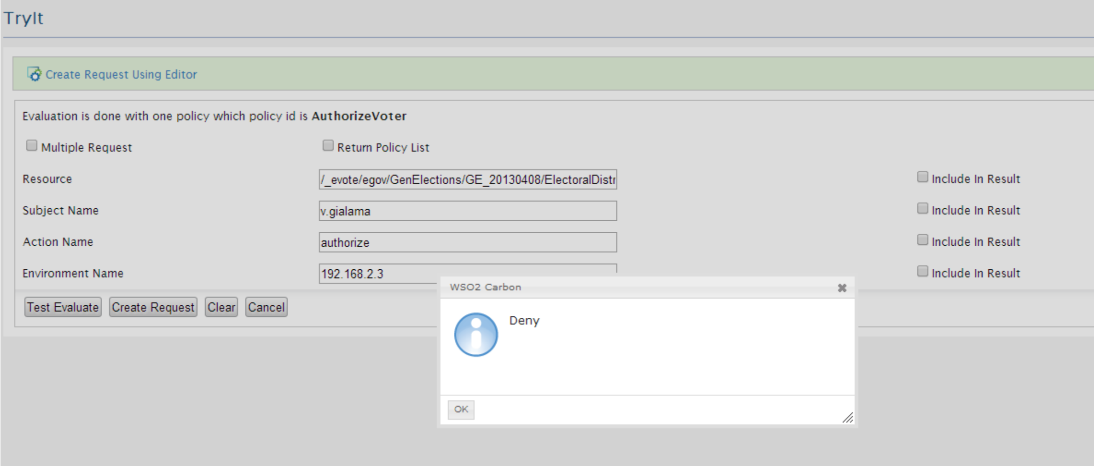
WSO2 Carbon

Permit

OK

Figure 20: Authorize Voter (Sucessful execution)

User	**v.gialama (IT Auditor)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots/Bal_00001.xml
Action	Authorize
Result	Deny



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **AuthorizeVoter**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistr □ Include In Result

Subject Name: v.gialama □ Include In Result

Action Name: authorize □ Include In Result

Environment Name: 192.168.2.3 □ Include In Result

Test Evaluate | Create Request | Clear | Cancel

WSO2 Carbon

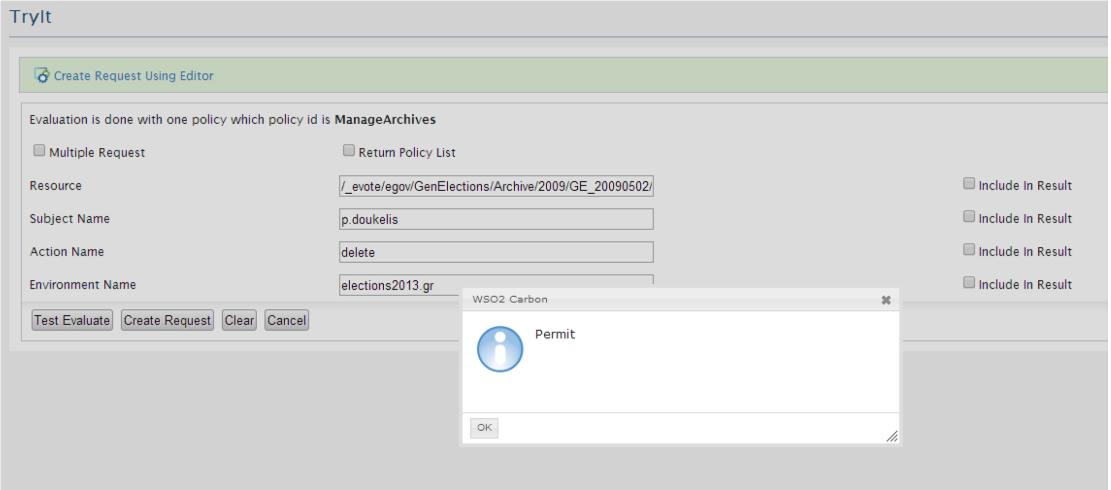
Deny

OK

Figure 21: Authorize Voter (Unsucessful execution)

5. *ManageArchives*: Election Organizers are eligible for writing, deleting the files of ballots or/and results corresponding to past elections. The domain must be ‘elections2013.gr’.

User	**p.doukelis (Election Organizer)**
Resource	/_evote/egov/GenElections/Archive/2009/GE_20090502/Ballots/AllBallots.xml
Action	Delete
Result	Permit


TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ManageArchives**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/Archive/2009/GE_20090502/ □ Include In Result

Subject Name: p.doukelis □ Include In Result

Action Name: delete □ Include In Result

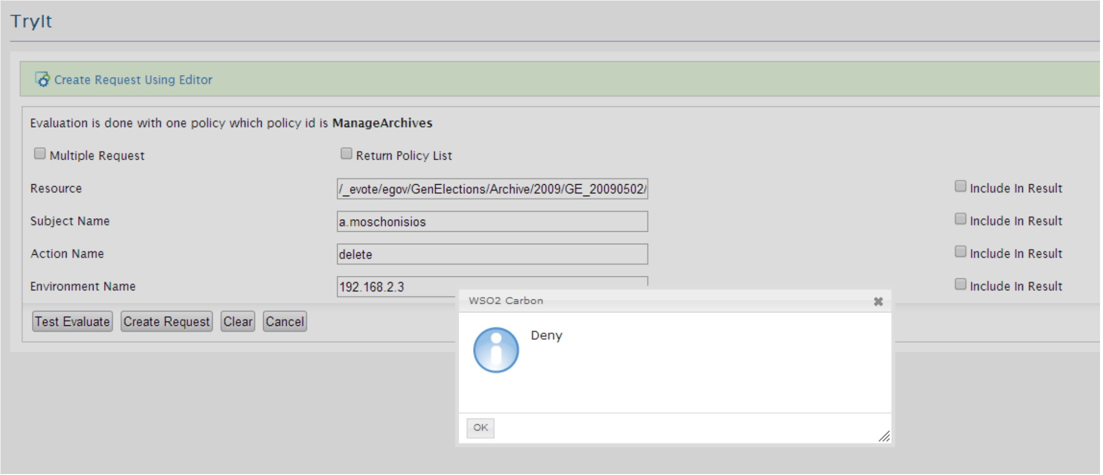
Environment Name: elections2013.gr □ Include In Result

WSO2 Carbon

Permit

Figure 22: Manage Archives (Sucessful execution)

User	**a.moschonisios(Party Representative)**
Resource	/_evote/egov/GenElections/Archive/2009/GE_20090502/Ballots/AllBallots.xml
Action	Delete
Result	Deny



Evaluation is done with one policy which policy id is **ManageArchives**

□ Multiple Request □ Return Policy List

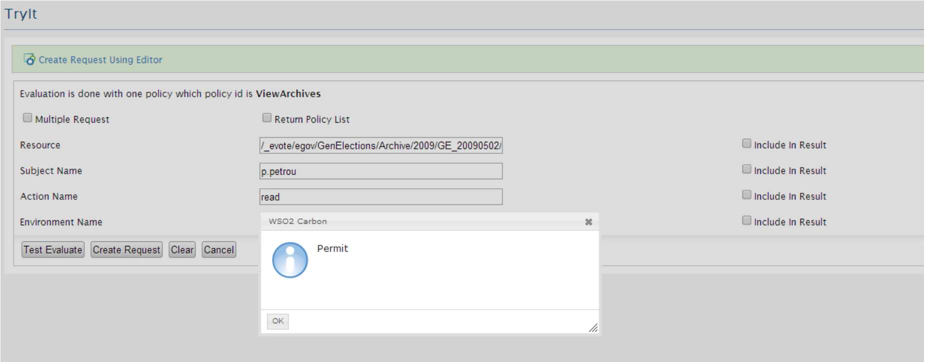
Resource	/_evote/egov/GenElections/Archive/2009/GE_20090502/	□ Include In Result
Subject Name	a.moschonisios	□ Include In Result
Action Name	delete	□ Include In Result
Environment Name	192.168.2.3	□ Include In Result

Deny

Figure 23: Manage Archives (Unsucessful execution)

6. *ViewArchives*: All users are authorized to view the archives of past elections.

User	**p.petrou (Voter)**
Resource	/_evote/egov/GenElections/Archive/2009/GE_20090502/Ballots/AllBallots.xml
Action	Read
Environment	-
Result	Permit



Evaluation is done with one policy which policy id is **ViewArchives**

□ Multiple Request □ Return Policy List

Resource	/_evote/egov/GenElections/Archive/2009/GE_20090502/	□ Include In Result
Subject Name	p.petrou	□ Include In Result
Action Name	read	□ Include In Result
Environment Name		□ Include In Result

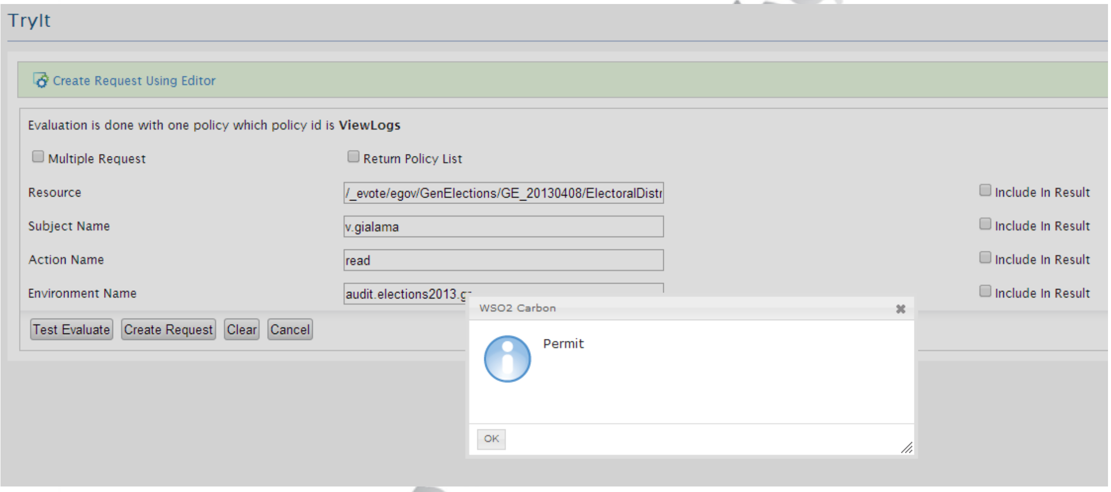
Permit

Figure 24: View Archives (Sucessful execution)

7. *ViewLogs*: IT Auditors are eligible for having read access to the log files of the electoral districts. This policy is applicable to all log files that correspond to the time

period the election process is active. The applicable domain that is allowed for this action is ‘*audit.elections2013.gr*’.

User	**v.gialama (IT Auditor)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Logs/previous/20130406.log
Action	Read
Result	Permit



Evaluation is done with one policy which policy id is **ViewLogs**

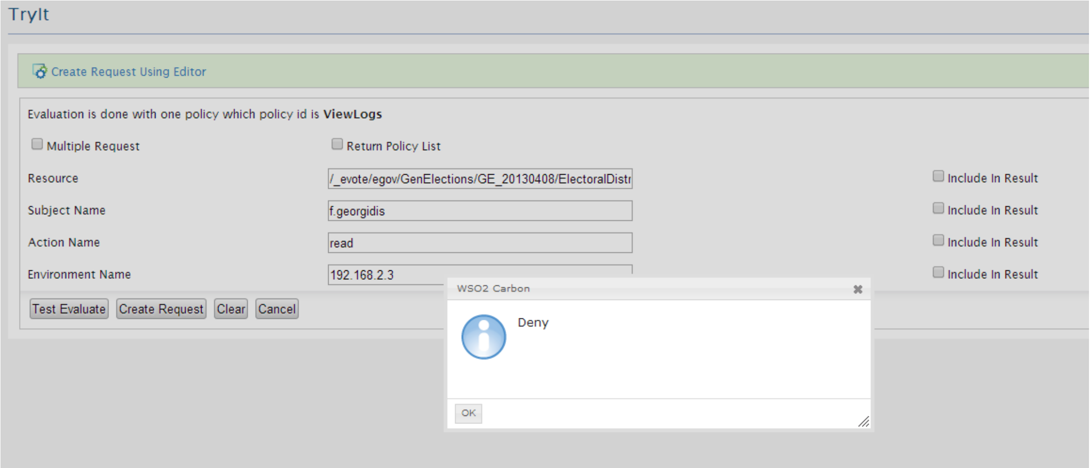
□ Multiple Request
□ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistri □ Include In Result
Subject Name: v.gialama □ Include In Result
Action Name: read □ Include In Result
Environment Name: audit.elections2013.g □ Include In Result

Permit

Figure 25: View Log Files (Sucessful execution)

User	**f.georgidis (Voter)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Logs/previous/20130406.log
Action	Read
Result	Deny



Evaluation is done with one policy which policy id is **ViewLogs**

□ Multiple Request □ Return Policy List

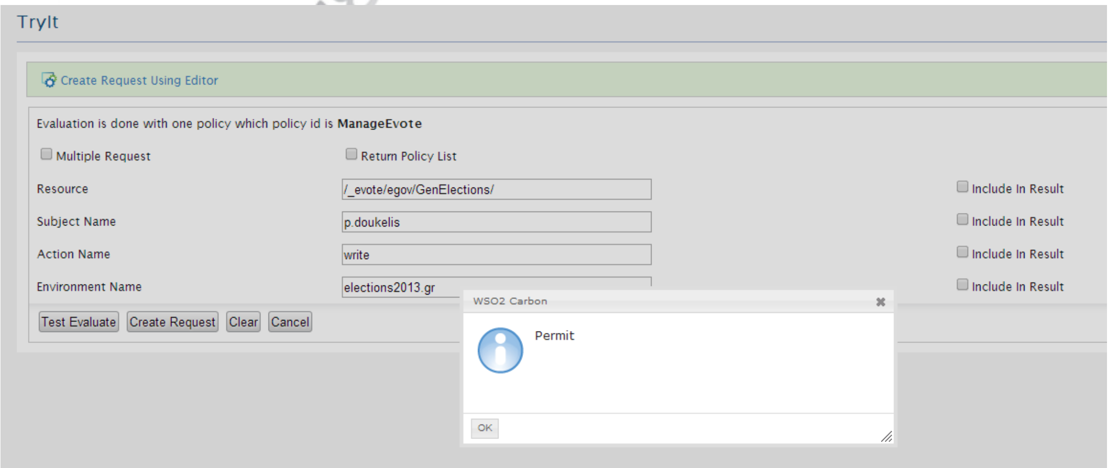
Resource /_evote/egov/GenElections/GE_20130408/ElectoralDistr □ Include In Result
Subject Name f.georgidis □ Include In Result
Action Name read □ Include In Result
Environment Name 192.168.2.3 □ Include In Result

Deny

Figure 26: View Log Files (Unsucessful execution)

8. *ManageEvote*: Election Organizers are eligible for reading, modifying and deleting items in the file system of ‘General Elections’ within the *evote* system.

User	**p.doukelis (Election Organizer)**
Resource	/_evote/egov/GenElections/
Action	Write
Result	Permit



Evaluation is done with one policy which policy id is **ManageEvote**

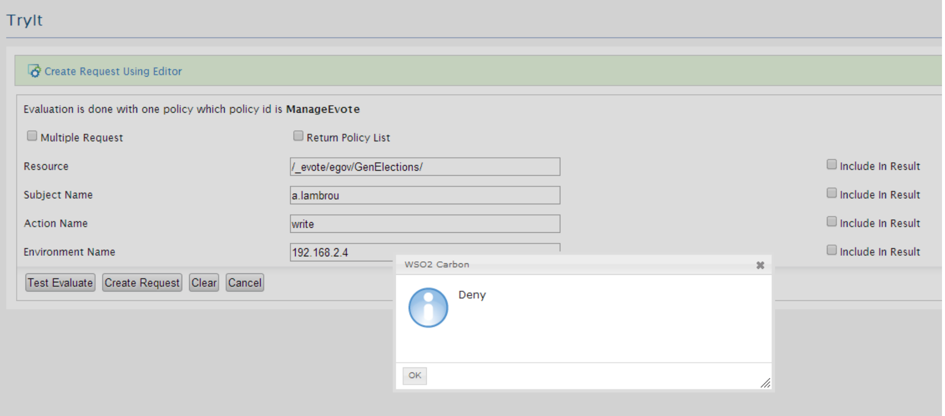
□ Multiple Request □ Return Policy List

Resource /_evote/egov/GenElections/ □ Include In Result
Subject Name p.doukelis □ Include In Result
Action Name write □ Include In Result
Environment Name elections2013.gr □ Include In Result

Permit

Figure 27: Manage Evote (Sucessful execution)

User	**a.lambrou (Party Representative)**
Resource	/_evote/egov/GenElections/
Action	Write
Result	Deny



TryIt

Evaluation is done with one policy which policy id is **ManageEvote**

□ Multiple Request □ Return Policy List

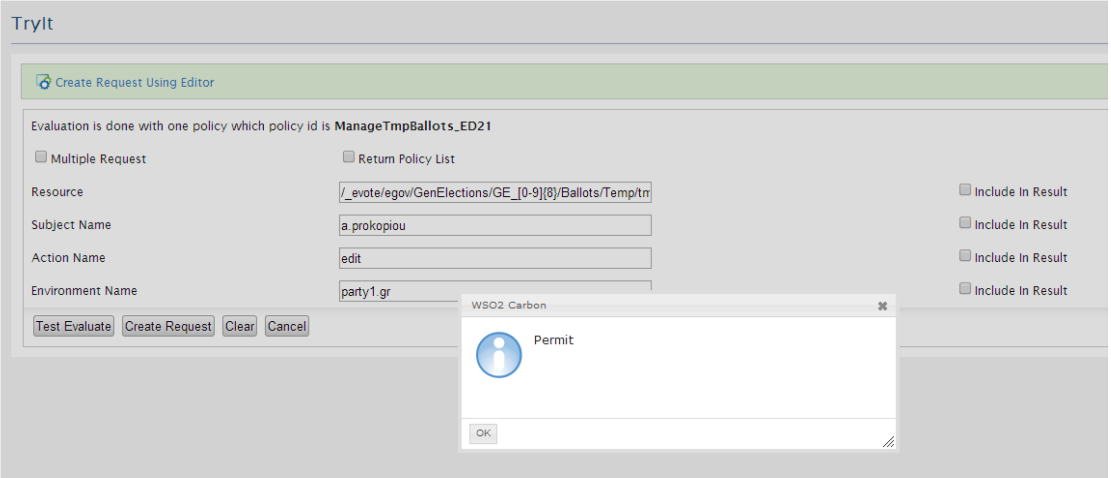
Resource	/_evote/egov/GenElections/	□ Include In Result
Subject Name	a.lambrou	□ Include In Result
Action Name	write	□ Include In Result
Environment Name	192.168.2.4	□ Include In Result

Deny

Figure 28: Manage Evote (Unsucessful execution)

9. *ManageTmpBallots_ED11:* Party Representatives belonging to the first party of the first electoral district, can modify the temporary ballot file of their party. The next policies perform the same check for the corresponding district/party. Note that the applicable domain that allows this action is ‘*party1.gr*’.
10. *ManageTmpBallots_ED12:* Party Representatives belonging to the second party of the first electoral district, can modify the temporary ballot file of their party. Note that the applicable domain that allows this action is ‘*party2.gr*’.
11. *ManageTmpBallots_ED21:* Party Representatives belonging to the first party of the second electoral district, can modify the temporary ballot file of their party. Note that the applicable domain that allows this action is ‘*party1.gr*’.

User	**a.prokopiou (Party Representative of 2nd electoral district and 1st party)**
Resource	/_evote/egov/GenElections/GE_20130408/Ballots/Temp/tmp_ED2_party1.xml
Action	Edit
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ManageTmpBallots_ED21**

□ Multiple Request □ Return Policy List

Resource	/_evote/egov/GenElections/GE_[0-9]{8}/Ballots/Temp/tm	□ Include In Result
Subject Name	a.prokopiou	□ Include In Result
Action Name	edit	□ Include In Result
Environment Name	party1.gr	□ Include In Result

Test Evaluate | Create Request | Clear | Cancel

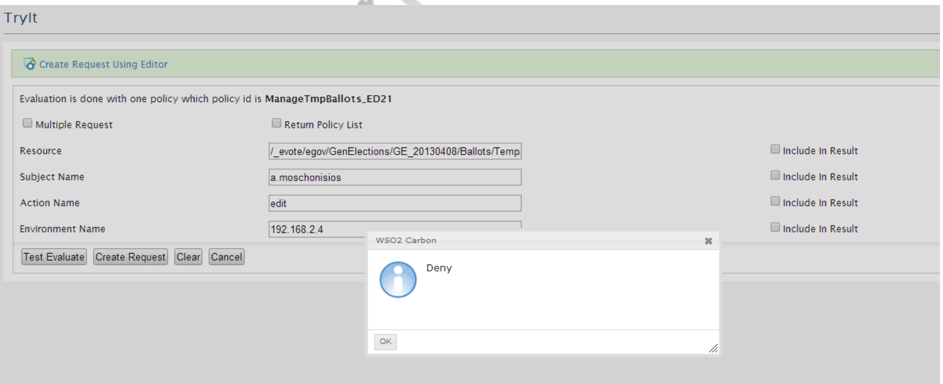
WSO2 Carbon

Permit

OK

Figure 29: Manage Temporary Ballots of 1st party for Electoral District 2 (Sucessful execution)

User	**a.moschonisios (Party Representative of 1st electoral district and 2nd party)**
Resource	/_evote/egov/GenElections/GE_20130408/Ballots/Temp/tmp_ED2_party1.xml
Action	Edit
Result	Deny



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ManageTmpBallots_ED21**

□ Multiple Request □ Return Policy List

Resource	/_evote/egov/GenElections/GE_20130408/Ballots/Temp.	□ Include In Result
Subject Name	a.moschonisios	□ Include In Result
Action Name	edit	□ Include In Result
Environment Name	192.168.2.4	□ Include In Result

Test Evaluate | Create Request | Clear | Cancel

WSO2 Carbon

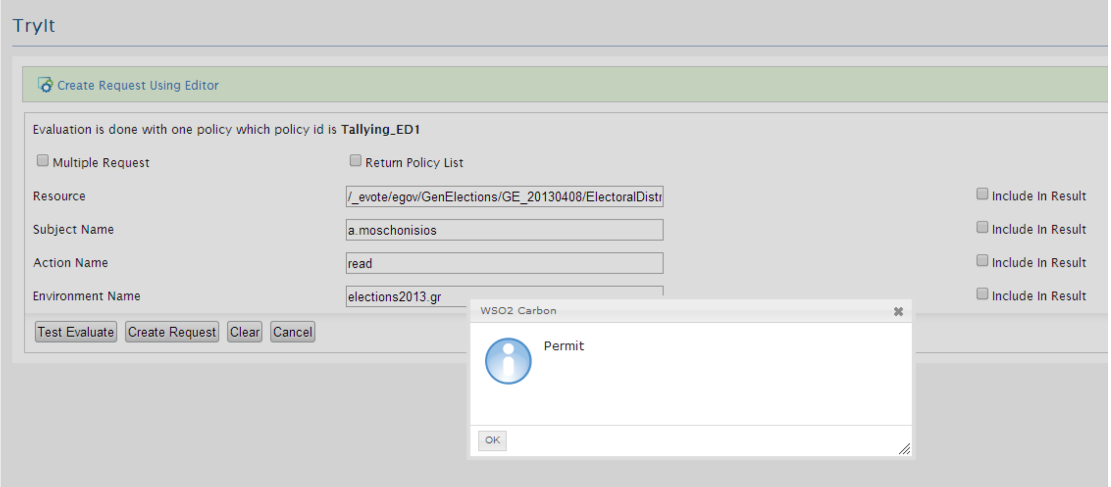
Deny

OK

Figure 30: Manage Temporary Ballots of 1st party for Electoral Distict 2 (Unsucessful execution)

12. *Tallying_ED1:* Election Organizers, IT Auditors, Party Representatives and system administrators are eligible for reading the Ballots Pool directory, in order to perform the tallying. In case of denied access, a message is issued to the user “You are not authorized for participating in tallying”.

User	**a.moschonisios (Party Representative of 1st electoral district and 2nd party)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots Pool/Bal_00010.xml
Action	Read
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **Tallying_ED1**

□ Multiple Request □ Return Policy List

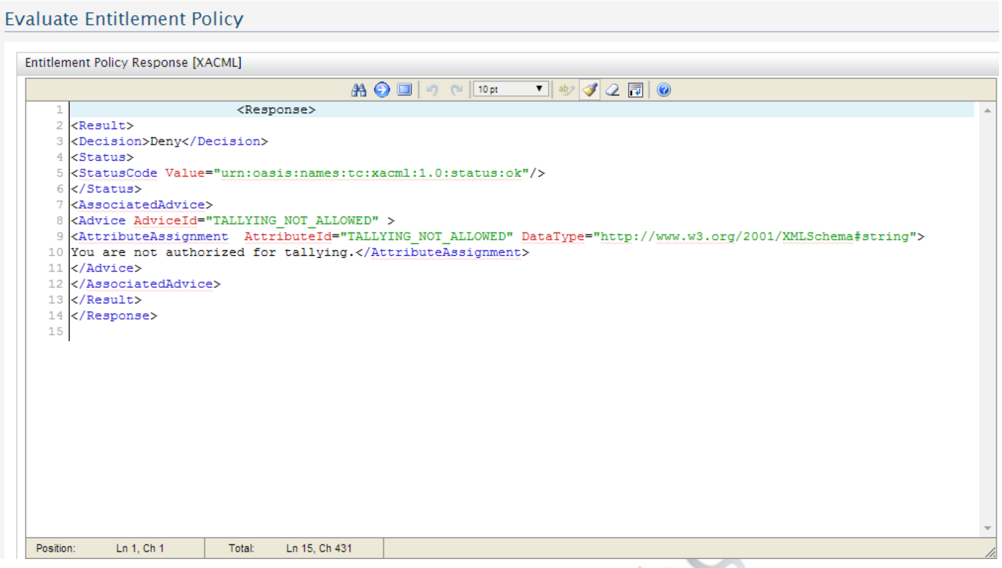
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistr	□ Include In Result
Subject Name	a.moschonisios	□ Include In Result
Action Name	read	□ Include In Result
Environment Name	elections2013.gr	□ Include In Result

WSO2 Carbon

Permit

Figure 31: Tallying for Electoral Distict 1 (Sucessful execution)

User	**f.georgidis (Voter)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots Pool/Bal_00010.xml
Action	Read
Result	Deny



Evaluate Entitlement Policy

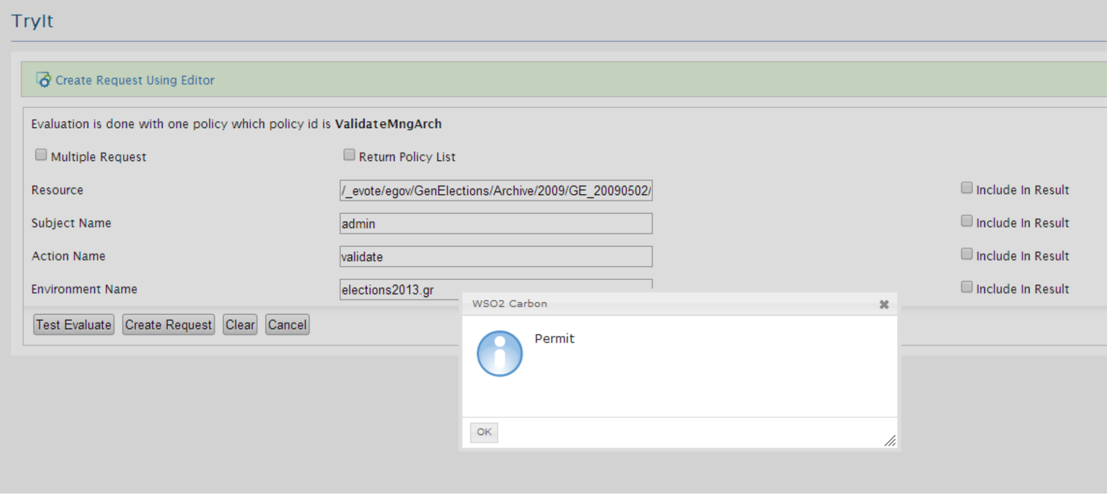
Entitlement Policy Response [XACML]

```
                    <Response>
<Result>
<Decision>Deny</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
<AssociatedAdvice>
<Advice AdviceId="TALLYING_NOT_ALLOWED" >
<AttributeAssignment  AttributeId="TALLYING_NOT_ALLOWED" DataType="http://www.w3.org/2001/XMLSchema#string">
You are not authorized for tallying.</AttributeAssignment>
</Advice>
</AssociatedAdvice>
</Result>
</Response>
```

Figure 32: Tallying for Electoral Distict 1 (Unsucessful execution)

13. *ValidateMngArch:* System administrator validates any modification in the *evote* archives.

User	**admin**
Resource	/_evote/egov/GenElections/Archive/2009/GE_20090502/Ballots/AllBallots.xml
Action	Validate
Result	Permit



TryIt

Evaluation is done with one policy which policy id is **ValidateMngArch**

□ Multiple Request □ Return Policy List

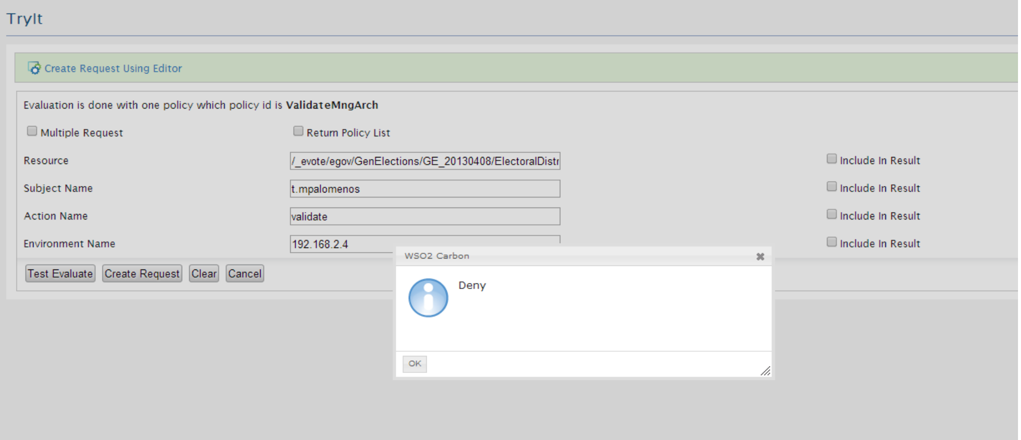
Resource	/_evote/egov/GenElections/Archive/2009/GE_20090502/	□ Include In Result
Subject Name	admin	□ Include In Result
Action Name	validate	□ Include In Result
Environment Name	elections2013.gr	□ Include In Result

WSO2 Carbon

Permit

Figure 33: Validate Archive Management (Sucessful execution)

User	**t.mpalomenos (Election Organizer)**
Resource	/_evote/egov/GenElections/Archive/2009/GE_20090502/Ballots/AllBallots.xml
Action	Validate
Result	Deny



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ValidateMngArch**

☐ Multiple Request ☐ Return Policy List

Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistr	☐ Include In Result
Subject Name	t.mpalomenos	☐ Include In Result
Action Name	validate	☐ Include In Result
Environment Name	192.168.2.4	☐ Include In Result

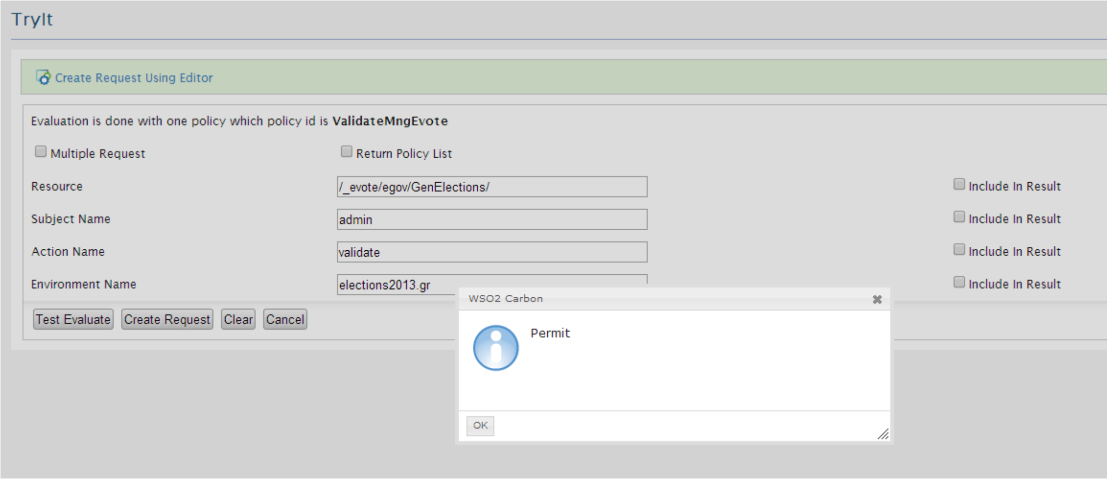
WSO2 Carbon

Deny

Figure 34: Validate Archive Management (Unsucessful execution)

14. *ValidateMngEvote:* System admin validates any modification in the General Elections file system.

User	**admin**
Resource	/_evote/egov/GenElections/
Action	Validate
Result	Permit


TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ValidateMngEvote**

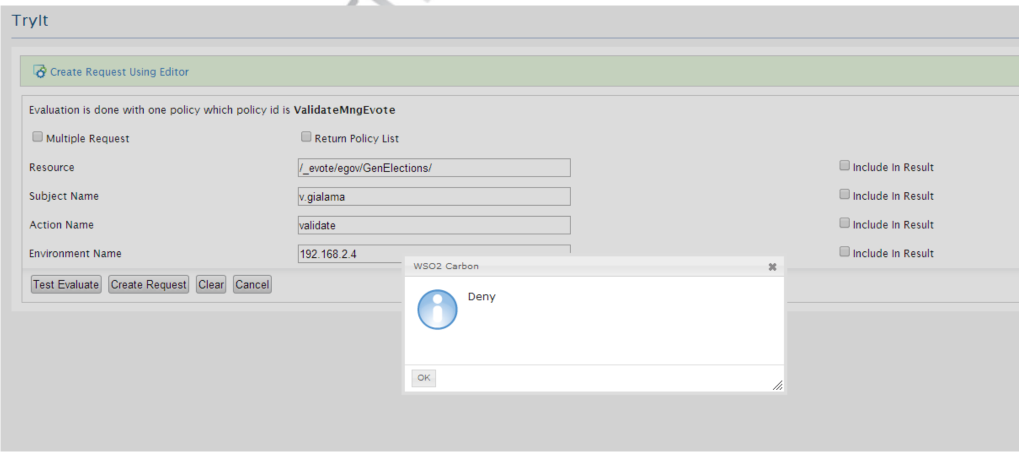
□ Multiple Request □ Return Policy List

Resource	/_evote/egov/GenElections/	□ Include In Result
Subject Name	admin	□ Include In Result
Action Name	validate	□ Include In Result
Environment Name	elections2013.gr	□ Include In Result

Permit

Figure 35: Validate Evote Management (Sucessful execution)

User	**v.gialama (IT Auditor)**
Resource	/_evote/egov/GenElections/
Action	Validate
Result	Deny


TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ValidateMngEvote**

□ Multiple Request □ Return Policy List

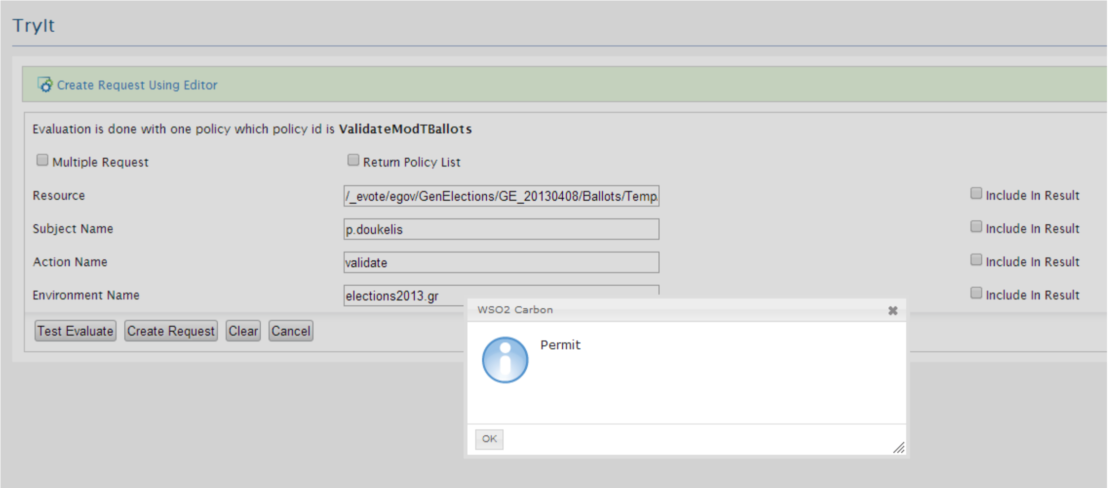
Resource	/_evote/egov/GenElections/	□ Include In Result
Subject Name	v.gialama	□ Include In Result
Action Name	validate	□ Include In Result
Environment Name	192.168.2.4	□ Include In Result

Deny

Figure 36: Validate Evote Management (Unsucessful execution)

15. *ValidateModTBallots*: Election Organizers validate any modification made in temporary ballot files.

User	**p.doukelis (Election Organizer)**
Resource	/_evote/egov/GenElections/GE_20130408/Ballots/Temp/tmp_ED1_party1.xml
Action	Validate
Result	Permit



Evaluation is done with one policy which policy id is **ValidateModTBallots**

□ Multiple Request □ Return Policy List

Resource /_evote/egov/GenElections/GE_20130408/Ballots/Temp □ Include In Result

Subject Name p.doukelis □ Include In Result

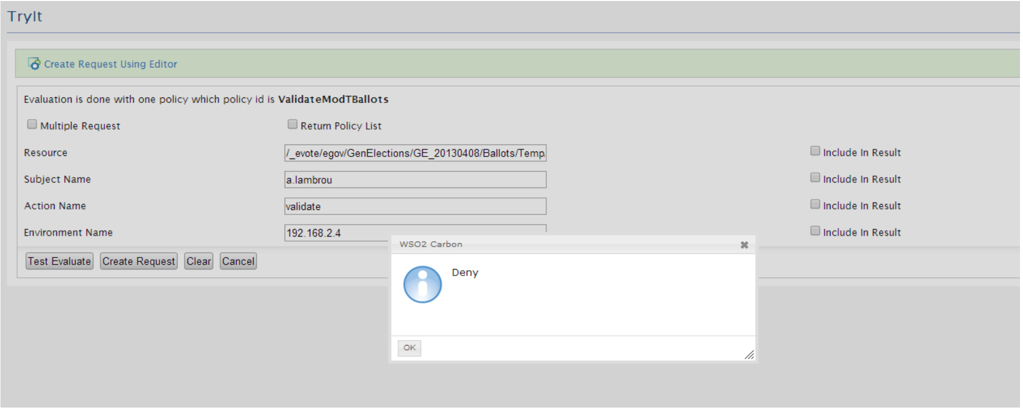
Action Name validate □ Include In Result

Environment Name elections2013.gr □ Include In Result

Permit

Figure 37: Validate Modifications to temporary ballot files (Sucessful execution)

User	**a.lambrou (Party Representative)**
Resource	/_evote/egov/GenElections/GE_20130408/Ballots/Temp/tmp_ED1_party1.xml
Action	Validate
Result	Deny



Evaluation is done with one policy which policy id is **ValidateModTBallots**

□ Multiple Request □ Return Policy List

Resource /_evote/egov/GenElections/GE_20130408/Ballots/Temp □ Include In Result

Subject Name a.lambrou □ Include In Result

Action Name validate □ Include In Result

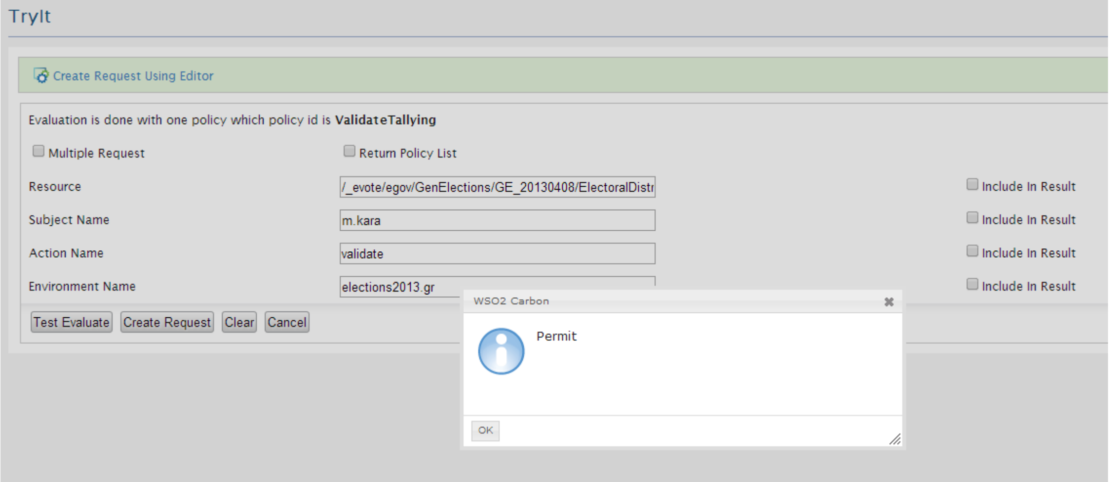
Environment Name 192.168.2.4 □ Include In Result

Deny

Figure 38: Validate Modifications to temporary ballot files (Unsucessful execution)

16. *ValidateTallying:* The outcome of the tallying process is subjected to validation from election organizers and system administrators.

User	**m.kara (Election Organizer)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Results/ED1_Results.xml
Action	Validate
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ValidateTallying**

□ Multiple Request □ Return Policy List

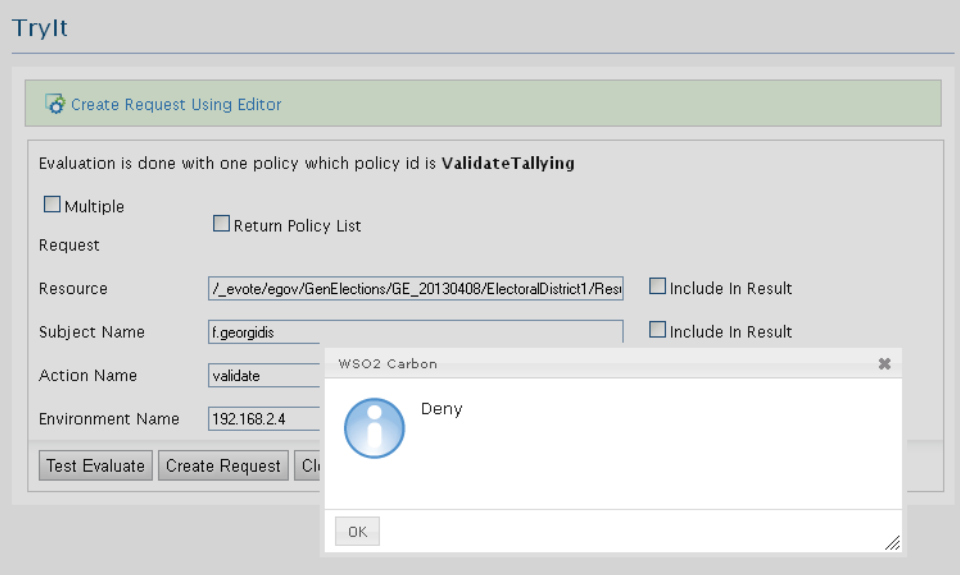
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistr	□ Include In Result
Subject Name	m.kara	□ Include In Result
Action Name	validate	□ Include In Result
Environment Name	elections2013.gr	□ Include In Result

WSO2 Carbon

Permit

Figure 39: Validate Tallying Results (Sucessful execution)

User	**f.georgidis (Voter)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Results/ED1_Results.xml
Action	Validate
Result	Deny



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ValidateTallying**

☐ Multiple Request

☐ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Resu ☐ Include In Result

Subject Name: f.georgidis ☐ Include In Result

Action Name: validate

Environment Name: 192.168.2.4

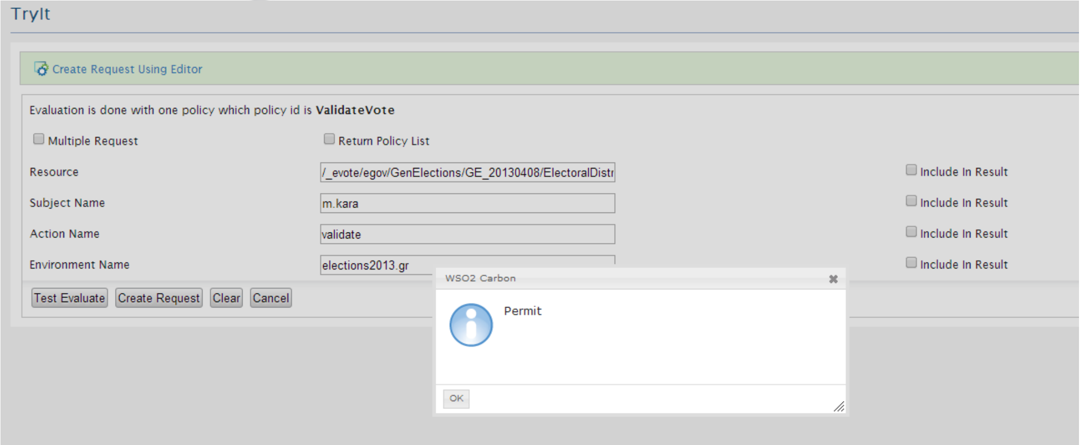
WSO2 Carbon

Deny

Figure 40: Validate Tallying Results (Unsucessful execution)

17. *ValidateVote:* Election Organizers are eligible for validating the modifications in the ballot files (voting process).

User	**m.kara (Election Organizer)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots/Bal_00001.xml
Action	Validate
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ValidateVote**

☐ Multiple Request

☐ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistr ☐ Include In Result

Subject Name: m.kara ☐ Include In Result

Action Name: validate ☐ Include In Result

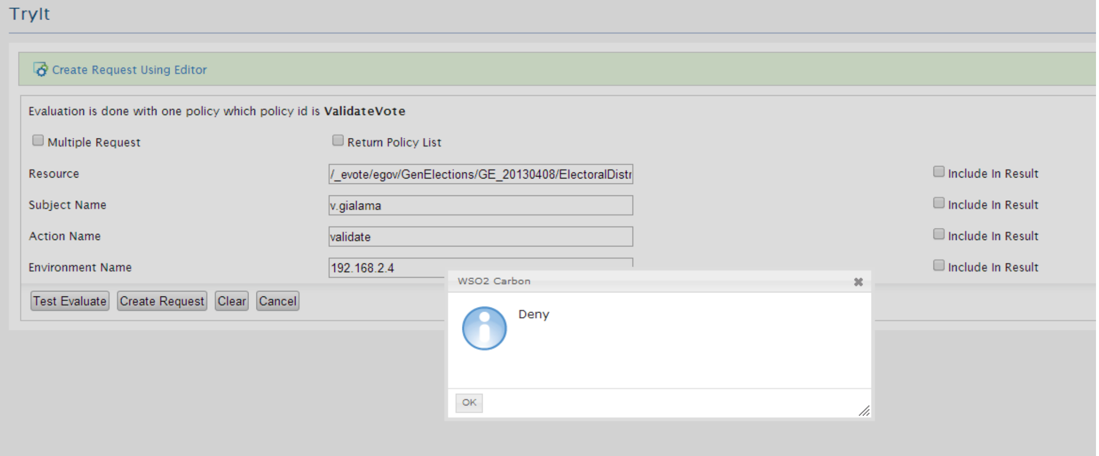
Environment Name: elections2013.gr ☐ Include In Result

WSO2 Carbon

Permit

Figure 41: Validate Voting (Sucessful execution)

User	**v.gialama (IT Auditor)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots/Bal_00001.xml
Action	Validate
Result	Deny


TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ValidateVote**

☐ Multiple Request ☐ Return Policy List

Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistr	☐ Include In Result
Subject Name	v.gialama	☐ Include In Result
Action Name	validate	☐ Include In Result
Environment Name	192.168.2.4	☐ Include In Result

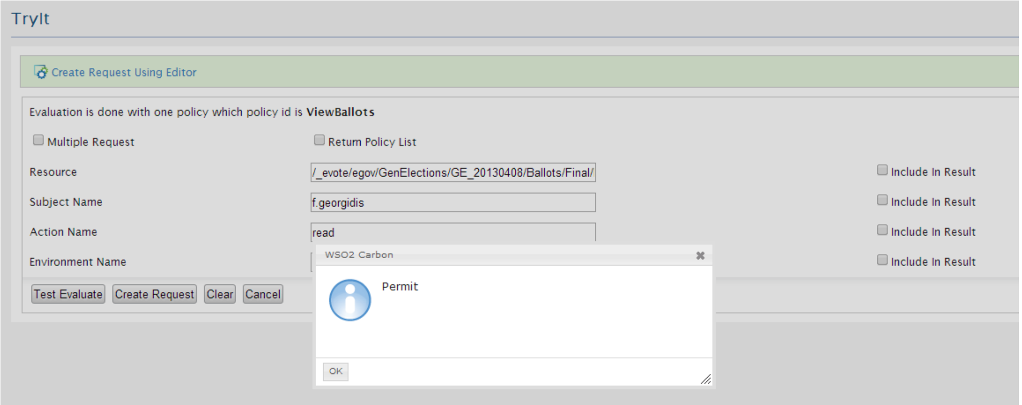
WSO2 Carbon

Deny

Figure 42: Validate Voting (Unsucessful execution)

18. *ViewBallots*: All users are authorized to view the ballot files of all election districts of all participating parties.

User	**f.georgidis (Voter)**
Resource	/_evote/egov/GenElections/GE_20130408/Ballots/Final/ED1/BA_ED1_party1.xml
Action	Read
Environment	-
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ViewBallots**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/Ballots/Final/ □ Include In Result

Subject Name: f.georgidis □ Include In Result

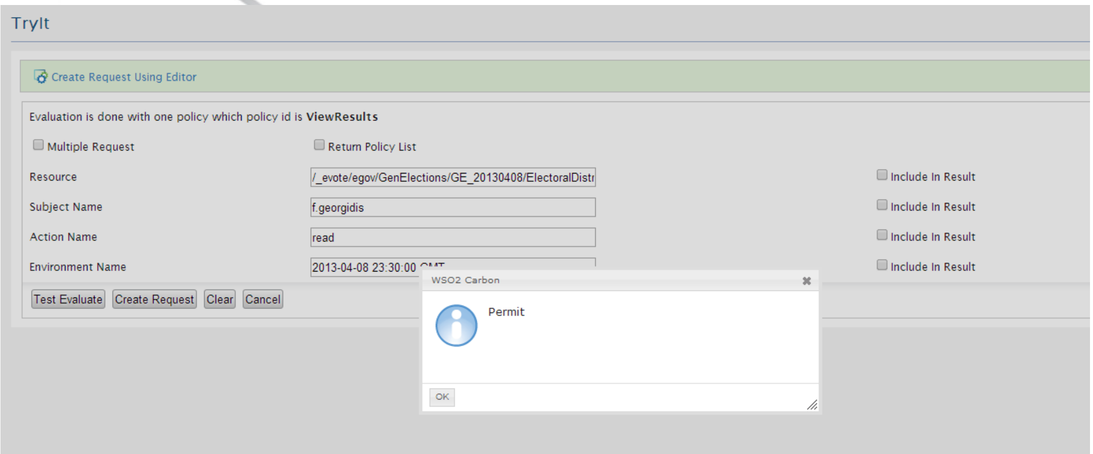
Action Name: read □ Include In Result

Environment Name: □ Include In Result

Figure 43: View Final Ballots (Sucessful execution)

19. *ViewResults*: All users are eligible for reading the result files of the current election process with the obligation that the election process must be closed (voting process and tallying). The process is considered completed after 23:00 o' clock of the 8th of April 2013.

User	**f.georgidis (Voter)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Results/ED1_Results.xml
Action	Read
Environment	2013-04-08 23:30:00 GMT
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **ViewResults**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistr □ Include In Result

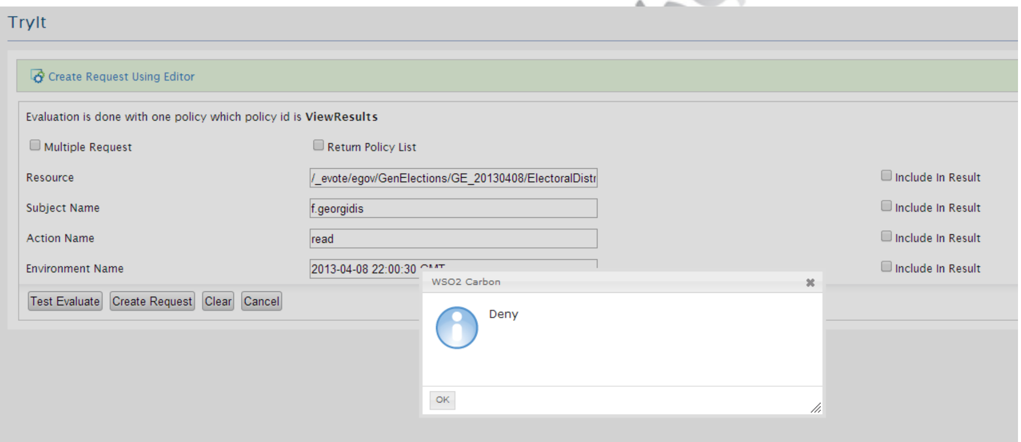
Subject Name: f.georgidis □ Include In Result

Action Name: read □ Include In Result

Environment Name: 2013-04-08 23:30:00 GMT □ Include In Result

Figure 44: View Results (Sucessful execution)

User	**f.georgidis (Voter)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Results/ED1_Results.xml
Action	Read
Environment	2013-04-08 22:00:30 GMT
Result	Deny



Evaluation is done with one policy which policy id is **ViewResults**

□ Multiple Request □ Return Policy List

Resource: /_evote/egov/GenElections/GE_20130408/ElectoralDistr □ Include In Result

Subject Name: f.georgidis □ Include In Result

Action Name: read □ Include In Result

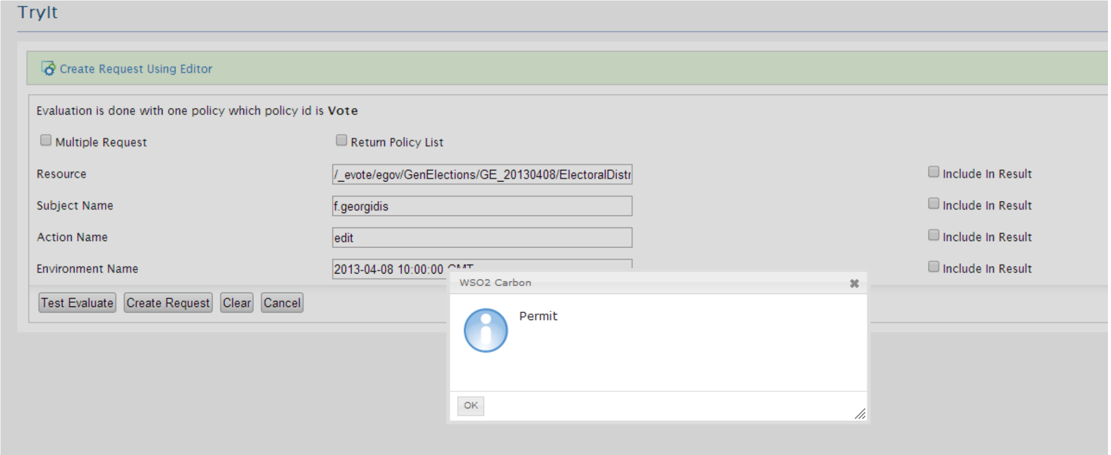
Environment Name: 2013-04-08 22:00:30 GMT □ Include In Result

Deny

Figure 45: View Results (Unsucessful execution)

20. *Vote*: Voters are authorized to edit their ballot files only in case they have not previously voted (Vote Flag = ‘0’) and the ballot file is the unique ballot file assigned to each user (Ballot ID).

User	**f.georgidis (Voter)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots/Bal_00005.xml
Action	Edit
Environment	2013-04-08 10:00:00 GMT
Result	Permit



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **Vote**

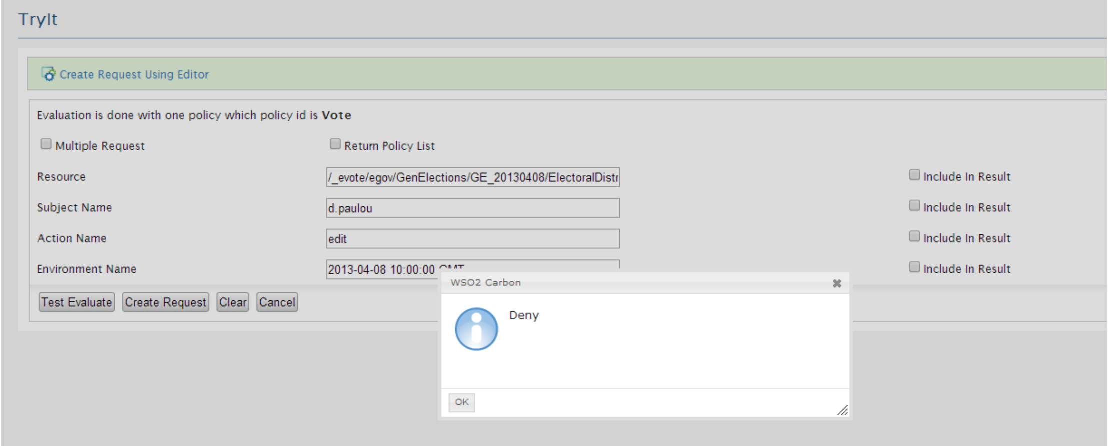
□ Multiple Request □ Return Policy List

Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistr	□ Include In Result
Subject Name	f.georgidis	□ Include In Result
Action Name	edit	□ Include In Result
Environment Name	2013-04-08 10:00:00 GMT	□ Include In Result

Permit

Figure 46: Vote (Sucessful execution)

User	**d.paulou (Voter)**
Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistrict1/Ballots/Bal_00005.xml
Action	Edit
Environment	2013-04-08 10:00:00 GMT
Result	Deny



TryIt

Create Request Using Editor

Evaluation is done with one policy which policy id is **Vote**

□ Multiple Request □ Return Policy List

Resource	/_evote/egov/GenElections/GE_20130408/ElectoralDistr	□ Include In Result
Subject Name	d.paulou	□ Include In Result
Action Name	edit	□ Include In Result
Environment Name	2013-04-08 10:00:00 GMT	□ Include In Result

Deny

Figure 47: Vote (Unsuccessful execution)

Conclusions

The expansion of e-government worldwide requires the review and redefinition of security measures used in such kind of applications. The criticality of the services as well as the impact of security breaches, demand the definition of security policies that will determine the access control to the system resources. However, embedded authorization permits users to perform a certain action without going through an access-control check from a third-party system which can lead to serious control issues. Moreover, with embedded authorization, it becomes virtually impossible to obtain a consolidated view of the policies protecting the various resources of enterprise applications. These security issues can be controlled by centralizing and shifting authorization decisions to a separate place and then accessing them whenever and wherever authorization decisions need to be made. The eXtensible Access Control Markup Language (XACML) technology presents a simple and powerful solution for doing so.

The OASIS standard for *fine-grained authorization management* introduces an architecture that performs the validation of a user's access on a resource. The XACML is a rich language that combines both role and attribute based access control. Hence, it does not rely only on subject, action and resource but on environment (time, place) as well.

The variety of features and functions that XACML supports, provide a platform that can be used by any system despite the nature of the information system. Also, the system's specificities can be handled since the user can make its own customizations that will satisfy the system's design requirements. Furthermore, the definition of policies, make the platform easily implemented and extensible on information systems.

According to the architecture introduced by the OASIS standard, XACML modules that evaluate access request can be used as a service. The feature of externalization is crucial, since organizations need to use the modules for access control, without embedding new software within their systems. Policy Enforcement Point sends the requests to Policy Decision Point where the actual evaluation of the requests is performed and the response is finalized.

The complexity of e-voting systems is associated to the variety of roles and functionalities that are provided to the users. Access control needs to filter the requests from subjects that request to perform an action to a resource. Also, the subject's attributes need to be taken into consideration in order the system to grant or refuse the action. The implementation part of the current thesis has proven that XACML standard can be used in order to provide a secure system according to the system and design requirements that were initially set.

Appendix

1. Indicative XML schema of Ballot file

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<evotebal id="00001">
<UserRole="Voter">
      <UserData>
            <ElectoralDistrict>ED1</ElectoralDistrict>
            <Party>0</Party>
      </UserData>
      <BallotData>
            <VoteParty>1</VoteParty>
            <Candidate1>Charitou F. Melpomeni</Candidate1>
            <Candidate2>Papadopoulos P. Panagiotis</Candidate2>
            <Candidate3>Legeonarios A. Aristos</Candidate3>
      </BallotData>
</User>
</evotebal>
```

2. User Roles mapping

The users defined within the system were assigned to particular roles in _evote. This mapping is depicted in the following table:

User	Role
admin	admin
m.kara	Election Organizers
p.doukelis	
t.mpalomenos	

v.gialama	IT Auditor
d.paulou	Voter
f.georgidis	
p.petrou	
v.pappa	
a.lambrou	Party Representatives
a.moschonisios	
a.prokopiou	

3. Policies – Source Code

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:ordered-permit-overrides" PolicySetId="EvotePS" Version="1.0">

<Description> The e-vote system Policy Set. </Description>

<Target/>

<PolicyIdReference>AuthorizeLogBrowse</PolicyIdReference>

<PolicyIdReference>AuthorizeTallying</PolicyIdReference>

<PolicyIdReference>AuthorizeTmpBallots</PolicyIdReference>

<PolicyIdReference>AuthorizeVoter</PolicyIdReference>

<PolicyIdReference>ManageArchives</PolicyIdReference>

<PolicyIdReference>ManageEvote</PolicyIdReference>

<PolicyIdReference>ManageTmpBallots_ED11</PolicyIdReference>

<PolicyIdReference>ManageTmpBallots_ED12</PolicyIdReference>

<PolicyIdReference>ManageTmpBallots_ED21</PolicyIdReference>

<PolicyIdReference>Tallying_ED1</PolicyIdReference>

<PolicyIdReference>ValidateMngArch</PolicyIdReference>

<PolicyIdReference>ValidateMngEvote</PolicyIdReference>

<PolicyIdReference>ValidateModTBallots</PolicyIdReference>

<PolicyIdReference>ValidateTallying</PolicyIdReference>

<PolicyIdReference>ValidateVote</PolicyIdReference>

<PolicyIdReference>ViewArchives</PolicyIdReference>

<PolicyIdReference>ViewBallots</PolicyIdReference>

<PolicyIdReference>ViewLogs</PolicyIdReference>
```

```
<PolicyIdReference>ViewResults</PolicyIdReference>

<PolicyIdReference>Vote</PolicyIdReference>

</PolicySet>

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="AuthorizeLogBrowse"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="AuthorizeLogBrowse-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">authorize</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>

<AttributeDesignator       AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"         DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="AuthorizeLogBrowse-R2">

<Target>

<AnyOf>

<AllOf>
```

```
<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">authorize</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>
```

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="AuthorizeTallying"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="AuthorizeTallying-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">authorize</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-
least-one-member-of">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>
```

```
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">admin</AttributeValue>

</Apply>

<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>



<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="AuthorizeTmpBallots" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="AuthorizeTmpBallots-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">authorize</AttributeValue>

<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
```

```
subject"          DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="AuthorizeVoter"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="AuthorizeVoter-R1">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">authorize</Attribu
teValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>
```

```
<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>
```

```
<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ManageArchives"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ManageArch-R1">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeVa
lue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
```

```
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"            DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="ManageArch-R2">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">delete</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
```

```
<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="ManageArch-R3">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>
```

```
<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="ManageArch-R4">

<Target>
```

```
<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">delete</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>
```

```
</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="ManageEvote" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ManageEvote-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
```

```
<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="ManageEvote-R2">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer</AttributeValue>

<AttributeDesignator      AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"          DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="ManageEvote-R3">

<Target>

<AnyOf>

<AllOf>
```

```
<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>
```

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ManageTmpBallots_ED11"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-unless-deny" Version="1.0">

<Target/>

<Rule Effect="Deny" RuleId="ManageTmpBallots1-R1">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">party1.gr</Attribu
teValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ED1</AttributeValu
e>
```

```
<AttributeDesignator  AttributeId="http://wso2.org/claims/elDistrict"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

<Rule Effect="Deny" RuleId=" ManageTmpBallots1-R2">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">party1.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">1</AttributeValue>

<AttributeDesignator       AttributeId="http://wso2.org/claims/party"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"       DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ManageTmpBallots_ED12"
```

```
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny" Version="1.0">

<Target/>

<Rule Effect="Deny" RuleId="ManageTmpBallots2-R1">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">party2.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
</Match>
</AllOf>
</AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ED1</AttributeValue>
<AttributeDesignator AttributeId="http://wso2.org/claims/elDistrict" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
</Apply>
</Apply>
</Condition>
</Rule>
<Rule Effect="Deny" RuleId="ManageTmpBallots2-R2">
<Target>
<AnyOf>
<AllOf>
<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">party2.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
```

```
<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">2</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/party" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="ManageTmpBallots_ED21" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny" Version="1.0">

<Target/>

<Rule Effect="Deny" RuleId="ManageTmpBallots3-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeValue>

<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">party1.gr</Attribu
teValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ED2</AttributeValu
e>
```

```
<AttributeDesignator  AttributeId="http://wso2.org/claims/elDistrict"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"            DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

<Rule Effect="Deny" RuleId="ManageTmpBallots3-R2">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">party1.gr</Attribu
teValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">1</AttributeValue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/party"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"        DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Tallying_ED1"
```

```
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="Tallying-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/_evote/egov/GenEl
ections/GE_[0-9]{8}/ElectoralDistrict[1-99]/Ballots Pool/Bal_[0-
9]{5}.xml</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ITAuditor</Attribu
teValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

</Rule>

<Rule Effect="Permit" RuleId="Tallying-R2">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/_evote/egov/GenElections/GE_[0-9]{8}/ElectoralDistrict[1-99]/Ballots Pool/Bal_[0-9]{5}.xml</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

</Rule>

<Rule Effect="Permit" RuleId="Tallying-R3">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/_evote/egov/GenEl
```

```
ections/GE_[0-9]{8}/ElectoralDistrict[1-99]/Ballots      Pool/Bal_[0-
9]{5}.xml</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">admin</AttributeVa
lue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

</Rule>
```

```
<Rule Effect="Permit" RuleId="Tallying-R4">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/_evote/egov/GenEl
ections/GE_[0-9]{8}/ElectoralDistrict[1-99]/Ballots Pool/Bal_[0-
9]{5}.xml</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">PartyRepresentativ
e</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
```

```
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

</Rule>

<AdviceExpressions>

<AdviceExpression AdviceId="TALLYING_NOT_ALLOWED" AppliesTo="Deny">

<AttributeAssignmentExpression AttributeId="TALLYING_NOT_ALLOWED">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">You are not
authorized for tallying.</AttributeValue>

</AttributeAssignmentExpression>

</AdviceExpression>

</AdviceExpressions>

</Policy>

--

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ValidateMngArch"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ValidateAddArch-R1">

<Target>

<AnyOf>

<AllOf>
```

```
<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">validate</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>
```

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">admin</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="ValidateAddArch-R2">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">validate</AttributeValue>

<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>
```

```
<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">admin</AttributeVa
lue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>
```

```
<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ValidateMngEvote"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ValidateMngEvote-R1">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">validate</Attribut
eValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
```

```
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">admin</AttributeVa
lue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ValidateModTBallots"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ValidateMTBallots-R1">

<Target>
```

```
<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">validate</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>
```

```
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer</AttributeValue>
<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
</Apply>
</Condition>
</Rule>
</Policy>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="ValidateTallying" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">
<Target/>
<Rule Effect="Permit" RuleId="ValidateTallying-R1">
<Target>
<AnyOf>
<AllOf>
<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">validate</AttributeValue>
```

```
<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-
least-one-member-of">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
```

```
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer</AttributeValue>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">admin</AttributeValue>

</Apply>

<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="ValidateVote" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ValidateVote-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">validate</AttributeValue>

<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
```

```
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">elections2013.gr</
AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ElectionOrganizer<
/AttributeValue>
```

```
<AttributeDesignator AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ViewArchives"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ViewArchs-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>
```

```
<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Internal/everyone</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="ViewArchs-R2">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>

<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>
```

```
</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Internal/everyone<
/AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ViewBallots"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ViewBallots-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeVal
ue>
```

```
<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Internal/everyone<
/AttributeValue>

<AttributeDesignator        AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ViewLogs"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ViewLogs-R1">

<Target>
```

```
<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">audit.elections2013.gr</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>
```

```
</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ITAuditor</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="ViewLogs-R2">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>
```

```
</AnyOf>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">audit.elections2013.gr</AttributeValue>

<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ITAuditor</AttributeValue>

<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>

</Apply>

</Condition>
```

```
</Rule>

</Policy>

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="ViewResults"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-unless-permit" Version="1.0">

<Target/>

<Rule Effect="Permit" RuleId="ViewResults-R1">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
greater-than">
```

```
<Apply  FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-
and-only">

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">2013-04-08
23:00:00 GMT</AttributeValue>

</Apply>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Internal/everyone<
/AttributeValue>

<AttributeDesignator       AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

</Policy>

<Policy        xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Vote"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-overrides" Version="1.0">
```

```
<Target/>

<Rule Effect="Permit" RuleId="Vote-R1">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

<Apply      FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-greater-than">

<Apply  FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>
```

```
</Apply>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">2013-04-08
07:59:00 GMT</AttributeValue>

</Apply>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">00005</AttributeVa
lue>

<AttributeDesignator AttributeId="http://wso2.org/claims/im"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject" DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

<Rule Effect="Permit" RuleId="Vote-R2">

<Target>

<AnyOf>

<AllOf>

<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-
match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeVal
ue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-less-
than">

<Apply  FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-
and-only">

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">2013-04-08
19:00:00 GMT</AttributeValue>

</Apply>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">00005</AttributeVa
lue>

<AttributeDesignator          AttributeId="http://wso2.org/claims/im"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
```

```
subject"            DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

<Rule Effect="Deny" RuleId="Vote-R3">

<Target>

<AnyOf>

<AllOf>

<Match  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeValue>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Match>

</AllOf>

</AnyOf>

</Target>

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>
```

```
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">0</AttributeValue>

<AttributeDesignator      AttributeId="http://wso2.org/claims/gender"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Condition>

</Rule>

<Rule Effect="Deny" RuleId="Vote-R4">

<Condition>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

<Apply   FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-
least-one-member-of">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">edit</AttributeValue>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">delete</AttributeValue>

</Apply>

<AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
```

```
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">

<Function    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
regexp-match"/>

<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">00005</AttributeVa
lue>

<AttributeDesignator          AttributeId="http://wso2.org/claims/im"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"           DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>

</Apply>

</Apply>

</Apply>

</Condition>

</Rule>

</Policy>
```

References

[1] Functional Requirements for a Secure Electronic Voting System – Spyros Ikonomopoulos, Costas Lamprinoudakis, Dimitris Gkritzalis, Spyros Kokolakis, Kostas Vassiliou, University of the Aegean, Athens University of Economics and Business

[2] Electronic Voting Systems: Security Implications of the Administrative Workflow - Costas Lamprinoudakis, Spyros Kokolakis, Maria Karuda, Vasilis Tsoumas, Dimitris Gritzalis, Sokratis Katsikas - Dept. of Information and Communication Systems Engineering University of the Aegean, Dept. of Informatics, Athens University of Economics and Business

[3] Building a Reliable e-Voting System: Functional Requirements and Legal Constraints - Costas Lamprinoudakis, Dimitris Gritzalis, Sokratis Katsikas - Dept. of Information and Communication Systems Engineering University of the Aegean, Dept. of Informatics, Athens University of Economics and Business

[4] Electronic Voting Systems: The Impact of 'System Actors' to the Overall Security Level - Costas Lamprinoudakis, Vasilis Tsoumas, Maria Karuda, Dimitris Gritzalis, Sokratis Katsikas - Dept. of Information and Communication Systems Engineering University of the Aegean, Dept. of Informatics, Athens University of Economics and Business

[5] Requirements Engineering for E-Voting Systems - Kevin Daimi, Katherine Snyder, and RobertJames(http://www.emich.edu/ia/pdf/research/Requirements%20Engineering%20for%20E-Voting%20Systems,%20Kevin%20Daimi,%20Katherine%20Snyder,%20and%20Robert%20James.pdf)

[6] Uncoercible Anonymous Electronic Voting - Chun-I Fan and Wei-Zhe Sun (http://www.researchgate.net/publication/221556617_Uncoercible_Anonymous_Electronic_Voting/file/79e41513018aaecfb2.pdf)

[7] Development of a General - Purpose E-Voting Server - De Su, Yuichi Goto, Jingde Cheng

[8] Anonymous Electronic Voting Protocol with Deniable Authentication for Mobile Ad Hoc Networks – Maede Ashouri - Talouki and Ahmad Baraani - Dastjerdi (http://www.sersc.org/journals/IJMUE/vol9_no1_2014/33.pdf)

[9] Adding Attributes to Role-Based Access Control - D. Richard KuhnEdward J. Coyne Timothy R. Weil – NIST (http://csrc.nist.gov/groups/SNS/rbac/documents/kuhn-coyne-weil-10.pdf)

[10] Attribute Based Access Control – NIST (Draft) (http://csrc.nist.gov/nccoe/Building-Blocks/NCCoE_ABAC_Building_Block_Draft_20140221.pdf)

[11] Electronic Voting System Security - Muhammad Adeel Javaid – Member Vendor Advisory Council, CompTIA

[12] An XML Security Framework that Integrates NIST RBAC, MAC and DAC Policies - Alberto De la Rosa Algarín Ph.D. Proposal

[13] NIST Role Based Access Control Standard - http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf

[14] Fast Semantic Attribute-Role-Based Access Control (ARBAC) - Leo Obrst, Dru McCandless, David Ferrella - The MITRE Corporation McLean VA, Colorado Springs CO - http://stids.c4i.gmu.edu/papers/STIDSPapers/STIDS2013_T18_ObrstEtAl.PDF

[15] Secure Access Control for Health Information Sharing Systems - Suhair Alshehri and Rajendra K. Raj - A Contextual Usage Control Model - Xiaofeng Luo, Lin Li, Wanbo Luo

[16] Authorization-Authentication Using XACML and SAML - Jake Wu and Panos Periorellis - School of Computing Science, University of Newcastle upon Tyne http://www.cs.ncl.ac.uk/publications/trs/papers/907.pdf

[17] Kaspersky Academy – A Collaborative access Control Model for E-Voting Systems - http://www.kaspersky.com/images/John_Ultra.pdf

[18] ABAC and RBAC: Scalable, Flexible and Auditable Access Management – NIST http://csrc.nist.gov/groups/SNS/rbac/documents/coyne-weil-13.pdf

Electronic References

[1] OASIS – Advancing Open Standards for the Information Society – XACML 3.0 specs http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf

[2] ISO/IEC 10181-3:1996 Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=18199

[3] Open Voting Consortium - http://www.openvotingconsortium.org/

[4] Axiomatics https://axiomatics.com/

[5] Wikipedia – The Free Encyclopedia http://en.wikipedia.org/